Health care

Compliance regulations can help to secure patient data.

ebook

An SC Magazine publication

The right stuff

Regulatory compliance has become a big part of a hospital's management and operations structure, reports Stephen Lawton.

Advances in wireless technology, database management and data protection, along with laws addressing the requirements for confidentiality of patient health information (PHI), are changing the ways health care facilities manage data. But malware attacks, such as the one that compromised computers at Kern Medical Center for more than two weeks this past summer, combined with a plethora of potential new data leaks, can wreck havoc on a hospital's computer systems.

This eBook will look at specific ways health care facilities, ranging from small clinics and offices to large, regional medical centers, can protect themselves from data losses due to cyberattacks, negligence and internal threats.

Security experts agree that the health care industry is currently trying to digest a variety of data security and related laws. Not only are hospitals and other health care facilities subject to such laws as the *Health Insurance Portability and Accountability Act (HIPAA) of 1996* and the *Health Information Technology for Economic and Clinical Health (HITECH) Act*, enacted as part of the *American Recovery and Reinvestment Act of 2009*, but publicly held companies are subject to multiple SEC-mandated laws and guidelines as well, such as *Sarbanes-Oxley Act (SOX) of 2002* and the Payment Card Industry Data Security Standard (PCI DSS).

Regulatory compliance has become a significant part of a hospital's management and operations structure. But not all aspects of compliance require a degree in law or accounting. Often it requires just some common sense.

IT professionals would do well in emulating doctors and researchers of infectious disease, says Robert Gezelter, a Flushing, NY-based security and software consultant with more than 30 years' experience. Gezelter says that considerable research conducted that demonstrates that the lack of appropriate hygiene in hospitals was responsible for the spreading of staph infections among patients. Researchers determined that among the many recommendations to stop these infections were two simple steps every employee could do: Wash their hands every time they entered a patient's room and use gloves.

Similar simple protections could be used on IT systems to significantly reduce data loss and the introduction of malware, Gezelter says. While virtually all networks have some type of perimeter control, such as firewalls, network managers should secure web pages within the perimeter. Simply by making every web page that a health care provider, clerk, accountant and all other employees access be a secure page using secure socket layer (SSL) or secure HTTP, along with requiring that each page have a signed certificate from a bona fide certificate authority, data security will be enhanced. Even if someone does access the network illegally, he says, they won't be able to access the data.

Often the data loss is not due to an outside attack, but rather to something more mundane, such as a lost laptop or thumb drive, a monitor that is turned so that patients can view records from other patients, or documents left in plain sight, he says. Improved processes and procedures, along with what Gezelter calls "data hygiene" (secured wireless networks and SSL-protected web pages and pervasive virtual private networks within the intranet), will dramatically reduce data loss. "This is not rocket science," he says.

Ensuring protection

Christopher Paidhrin is not only the IT security and compliance officer for Southwestern Washington Medical Center (SWMC) in Vancouver, Wash., he also is a security evangelist and popular speaker at conferences about improving data security at health care facilities.

Health care

512m

data records have been breached in the United States since 2005

Paidhrin says that the best way to secure data is to have an informed and trusted staff that is empowered to take action to ensure security. Everyone on the staff, from top executives to housekeepers and clerks, are trained to look for potential security breaches and to take action to stop them immediately, he says.

> "You need to create a culture of caring and excellence."
> – *Christopher Paidhrin, Southwestern Washington Medical Center*

Education is the key, Paidhrin says, as is making security part of the DNA of the workplace. For example, supplemental, web-based training is not one-size-fits-all. Employees in every department get customized computer-based training that is designed for their specialty. Every employee must get a perfect score on every test annually, he says. If an employee is unsuccessful on a test, they can retest again. If the employee is unsuccessful in getting a top grade within 30 days, they get a verbal notice. If they still have not completed all of their tests at the 100 percent level after 60 days, they get a written notice. If, after 90 days, they still have not passed all of their tests at the 100 percent mark, they are terminated, regardless of their position as a staffer, provider or executive.

"You need to create a culture of caring and excellence," Paidhrin says.

One of the challenges hospitals face in creating that culture is getting everyone to buy in. Traditionally, "Doctors were king," says Eric Cole, author of several books on data security and CEO and chief scientist of Secure Anchor Consulting Systems in Reston, Va. Physicians who carried large grants with them could dictate how much inconvenience they would put up with before taking their grants to a different hospital. As a result, Cole says, security measures need to be transparent to the doctors. Additionally, doctors need to be persuaded that security and compliance are in their best interests.

However, managing the IT environment and enforcing IT regulations can cause a conflict of interest. One way to ensure compliance with a hospital's security directives is to have a separate group of individuals responsible for running IT operations and analyzing audit reports, Cole says. Separating responsibilities eliminates any opportunity for reports to be modified by the operations staff.

Cole acknowledges that personal health information (PHI) can be compromised by internal or external attackers. While firewalls and other technology can protect the perimeter, audit logs that are regularly analyzed are critical to monitoring internal abuse.

A hospital might have 80,000 patient records to which a doctor needs access, Cole says, but they would not access all of the records at the same time. Based on experience, doctors normally cannot deal with more than 10 patients a day, he says. If someone is accessing 15 or 20 charts a day, there is a chance, he says, that data is being accessed inappropriately. By setting triggers to go off if a single individual accesses more than 10 charts in a 24-hour period, for example, it becomes easier for the security team to track extraordinary activity in the database and separate valid inquiries from questionable ones.

In the past, paper files were difficult to steal from hospitals. Crooks had to photocopy a chart or physically remove paper, which could easily be seen, he says. Today, a USB drive can hold thousands of files and be impossible to see if someone walks out the door with one in their pocket.

One way of reducing this risk of data loss is to limit the type of data held on computer systems. By reducing the number of systems that hold PHI and restricting access to those systems, sensitive data cybersprawl can be reduced. "Sixty percent of all systems [in a hospital] don't need PHI," he says. By removing PHI from systems throughout a medical

18

personal identifiers must be treated with special care according to HIPAA.

Caring: Improving awareness

Southwestern Washington Medical Center (SWMC) in Vancouver, Wash., soon to change its name to Peace Health, has a program called Awareness in Depth that specifically is designed to improve employee understanding and cooperation in data security. Among the program's key components are:

- Multiple applicant screening criteria
- Rigorous interviewing processes
- New employee orientation
- Confidentiality and privacy agreements
- Policies, procedures and pocesses
- Appropriate use and access monitoring
- Departmental and computer-based training
- Annual, mandatory, web-based training modules
- IT security, privacy, appropriate use
- Annual "MUMs The Word" campaign
- *HIPAA*, confidentiality and IT security

The goal is to establish a culture of caring and excellence, says Christopher Paidhrin, SWMC's IT security and compliance officer.

center, the security staff can improve its ability to protect private data loss and enhance compliance.

Security consultant Lawrence Walsh, president and CEO of the 2112 Group, says CISOs in charge of IT at businesses in the health care field, should consider the physicians' vow (often incorrectly attributed to the Hippocratic Oath): "First, do no harm." CISOs need to focus on ways they can keep private records from becoming public, and Walsh recommends internal *and* external audits.

"Encryption is not a failsafe for compliance," he says. Although the traditional definition of perimeter security might have changed as more people get access to PHI, the model is not dead. Rather, it is necessary for the owner of the PHI to protect the data flow, ensuring that as it moves from one location to another, its integrity is not compromised.

Selling security

While Walsh says data leakage prevention (DLP) and other advanced security technologies are useful for protecting information, the flip side to security is access. True data security becomes a yin and yang struggle of protection versus inconvenience. For example, while using a token might add a layer of security for data access, it is not necessarily always the best choice for every situation. If the token itself becomes a contentious issue among doctors who might lose their token or forget it at home versus IT staff that enforce the token security, then the smooth running of the hospital could be put at risk.

Selling the idea of data security and greater inconvenience to the providers and researchers is not a question of legal compliance or data disclosure, Walsh says, but rather the issue of personal liability. When everyone in the security chain realizes they might have a personal liability if PHI is disclosed, the individuals involved tend to be more security-conscious.

Larry Whiteside, CISO for the Visiting Nurse Service of New York, agrees with Walsh that DLP provides the best policy options at this point, but Whiteside does not like to talk about "compliance" per se. Instead, he mentions building a security system on a framework that maps back to the compliance mandate. By building to the provisions, he says, the system will be secure and in compliance.

In building to the mandate, he says, the data's perimeter will expand to encompass all who need access, including everyone within

60%

of all systems [in a hospital] don't need PHI.

– Eric Cole, CEO and chief scientist, Secure Anchor Consulting Systems

the health care organization, as well as business partners who must also put in place the identification and access management control policies dictated by the owner of the PHI. Today, he says, an offsite partner is generally the weakest link.

Health care providers need to control PHI and hold their business partners contractually liable to meet the providers' security needs, not necessarily the security levels the partner believes are sufficient.

> "Health care providers need to dictate how to protect data."
> *– Larry Whiteside, CISO, Visiting Nurse Service of New York*

"[The health care providers] need to dictate how to protect the data," Whiteside says. "We need to conduct proactive audits to build on this." These audits could include the use of penetration testing, similar to the testing required in the PCI DSS guidelines. "If you have a successful penetration test against an application, it is a problem," he says. "It is not theoretical. It is real."

The simplest way of protecting PHI is user awareness, he says. Just as the public has learned over time that coughing into the elbow is better at keeping germs from spreading than coughing into one's hand, employees within health care facilities can learn how to keep private data safe.

Data security includes a variety of disciplines in today's health care facility, says Barry Stutler, owner of Baryxon LLC, an IT consultancy based in Sarasota, Fla. Combining biometrics, such as a fingerprint pad or eye scanner, along with RFID tags or a swipe-card reader, can enhance security as well. For facilities where individuals might need access to specific data, the IT department can house that data in a specific room protected by a biometric lock combined with a swipe card to provide access, he says. An RFID tag in the user's identification card could be programmed for proximity logon and logoff functions for computers within that room, limiting the inconvenience to the users but maximizing security.

Authentication versus authorization

A key challenge health care providers face when protecting data is authentication versus authorization. While someone might be *authorized* to see protected data, the hospital, for example, needs to make sure they are *authenticated* first. Conversely, just because an employee is authenticated, it does not mean that they automatically have the right to access the data they seek.

It is not just the provider personnel that require authentication and authorization; patients need to be authenticated as well. It is not sufficient just to know a patient's name. Even uncommon names could lead to mix-ups, resulting in incorrect medications or procedures done to the wrong patient.

While birth dates are a common way of authenticating patients, security consultant Gezelter says it is also useful to have iris scans and pictures of the patient. It also is critical that health providers read the charts and compare the records to the patients in the room. He says that if a patient is listed in the chart as taking medication for a disease or condition specific to a woman, for example, the clinician should not simply believe they have the right chart if the patient in the room is male.

Just because the computer says you have the right patient, it doesn't mean you do, he adds. Similarly, just because a patient has an insurance card, it does not mean the person is who they say they are or authorized to get care using that card.

Identifying patients is more than just a formality in some hospitals, it can be a major challenge. William Fawns, CIO at Kern Medical Center (KMC) in Bakersfield, Calif., says a big challenge is making sure that the person who comes into the center for service is indeed

100k

patients a year in the United States are killed by preventable medical errors.

– Institute of Medicine

Securing the facility: Tips for protection

Larry Whiteside, CISO for the Visiting Nurse Service of New York, offers three basic rules for protecting security in health care facilities.

- Use static IP addresses for users who need to access data on the network from outside the health care facility's firewall. By requiring static IP addresses and using virtual private networks, rules can be set to reduce the possibility of someone from the outside breaking through.
- Require third-party vendors and partners to undergo security audits. These audits should be conducted at least annually, if not more often. By proactively auditing partners that have access to PHI, a health care provider can ensure it has done its best to protect data.
- Establish and enforce policies for mobile devices. A considerable amount of data can be protected simply by ensuring that there are rules about laptops, phones, thumb drives, iPods and other mobile devices. These policies should include the ability to wipe data remotely if a device is lost that contains protected data.

who they say they are. Bakersfield is in California's Central Valley, one of the state's primary agricultural regions and home to a large number of undocumented workers. In many cases, Fawns says, patients at the hospital have either inadequate identification or none at all. However, Kern Medical Center is a county-run facility and, by law, cannot turn away anyone who asks for care.

In some cases, he says, someone who either does not have health insurance or perhaps is an undocumented worker living in the country illegally, will use the insurance card of a relative or acquaintance to get care. It is difficult to authenticate patients simply by asking questions, he says. Privacy laws limit the kinds of questions a hospital can ask and, in the case of individuals who are in the country illegally, the answers they provide might be designed to mask their residency status.

The hospital does not contact the U.S. Bureau of Citizenship and Immigration if it has concerns about a patient's immigration status, Fawns says. It is important that undocumented aliens understand this, but often they either do not believe it or ever learn about it.

If the patient is not authenticated and simply processed as the person whose name is on the insurance card, he says, the patient could get medication to which they have an allergy, a medical reason not to take the drug, or some other mitigating reason why that drug should not be prescribed. Additionally, the medical records would then show the person whose card was used was treated for an ailment they did not have, possibly causing complications for them in the future.

Fawns says it is essential for health care organizations to include security as a key component of discussions that include executive leadership. At Kern Medical Center, for example, the CIO meets regularly with other top executives, including the chief medical officer, chief nursing officer, chief operating officer and the chief executive officer.

Security is for everyone, he says. If doctors are discussing a patient's care in a public area such as an elevator, for example, and a housekeeper is also on the elevator, that staffer is authorized to remind the doctors that this discussion needs to be done in private. Similarly, if a hospital staffer sees a patient throw away post-surgery instructions that might contain PHI, that staffer is required to use proper precautions to retrieve that document and take it to a shredder.

At the Kern Medical Center, Fawns faces additional challenges not found in some pri-

7-20m

illegal immigrants are estimated to be living in the United States

– The Christian Science Monitor

vate hospitals. KMC is a teaching hospital affiliated with the University of California, Los Angeles (UCLA) and the University of California, Irvine (UCI). As such, patient data is analyzed for research purposes.

The hospital protects the patients' privacy by "de-identifying" the medical records and adding a random identifier when making them available to researchers. This way, researchers can view detailed medical records without identifying the patient involved. Should a researcher require additional information, such as talking directly to the patient, they must submit a request to the chief medical officer before gaining access to the private patient data.

KMC, like the Southwestern Washington Medical Center, uses supplemental computer-based training designed for specific jobs to improve the data security at the hospital. However, unlike its Washington counterpart, employees are not required to meet the perfect score threshold or face termination, Fawns says. Both hospitals have union employees, and much of the testing is required to comply with state regulations and Joint Commission rules.

Fawns is keenly aware of what can happen if security is breached. During the summer of 2010, Fawns spent 16 days working to rid the hospital servers and workstations of malware. He says the hospital has learned several lessons from the attack.

For one, operating system diversity is key. If you have Windows-based desktop systems, then use Linux-based servers, he says. That way malware cannot move from desktop to desktop since the server will be a different OS.

Also useful is diversity in anti-virus and anti-malware software. Different brands often will find different viruses. If a hospital standardizes on only one type, then attacks that are designed to get past that brand can affect the hospital's systems.

Further, when repairing systems that have been breached, start from the inside and work out, Fawns says. Cleaning the servers first will lead to the greatest and fastest impact. After the servers, clean the thin clients before going after the Windows-based PCs. Even if some users say they have priority, such as an executive or other individual user, these individual's workstations should be placed behind the primary and application servers in priority. Cleaning workstations before the servers also can be counterproductive if the servers continue to reinfect the workstations.

Focus on the patient-centric systems and leave administrative systems for the end, Fawns says.

While security experts agree that compliance can be a daunting task, common sense and simple policies and procedures can dramatically reduce the potential for lost data. Practicing smart *data hygiene* and enforcing existing rules about protecting private health information can reduce compliance costs and improve data security without dramatically increasing IT expenditures. ■

For more information about ebooks from SC Magazine, *please contact Illena Armstrong, editor-in-chief, at illena.armstrong@haymarketmedia.com.*

$6b

is the price data breaches of patient information cost health care organizations in the United States each year.

– Ponemon Institute

Sponsors

GeoTrust® is the world's second largest digital certificate provider. More than 100,000 customers in over 150 countries trust GeoTrust to secure online transactions and conduct business over the Internet. Our range of digital certificate and trust products enable organizations of all sizes to maximize the security of their digital transactions cost-effectively.

DigitalPersona is a global provider of authentication and endpoint protection solutions that make security simple, practical and affordable for businesses of all sizes. The company helps enterprises, government agencies, custom application developers and independent software vendors to efficiently address growing security, compliance and fraud-prevention demands. DigitalPersona's award-winning technology is offered by market-leading computer manufacturers and solution providers around the world. *For more information, contact DigitalPersona at +1 650.474.4000, or visit www.digitalpersona.com.*

CREDANT is the trusted expert in data protection. Founded in 2001, CREDANT enables health care organizations to control, manage and protect data on vulnerable laptops, desktops, PCs, Macs, smartphones and removable media devices. Protecting sensitive information on seven million endpoints, CREDANT provides the most comprehensive mobile data protection and management platform.
For more information, visit www.credant.com.

Masthead

EDITORIAL

EDITOR-IN-CHIEF Illena Armstrong
illena.armstrong@haymarketmedia.com

EXECUTIVE EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com

MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION

ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com

SENIOR PRODUCTION Krassi Varbanov
krassi.varbanov@haymarketmedia.com

U.S. SALES

EASTERN REGION SALES MANAGER Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*

WESTERN REGION SALES MANAGER Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

SENIOR SALES EXECUTIVE Brittany Thompson
(646) 638-6152 *brittany.thompson@haymarketmedia.com*

SALES/EDITORIAL ASSISTANT Brittaney Kiefer
(646) 638-6104 *brittaney.kiefer@haymarketmedia.com*

Jackson Hospital Case Study

LOCATION

Montgomery, AL

OVERVIEW

Jackson Hospital is one of the largest not-for-profit community hospitals in Alabama. To improve the efficiency of staff at the point of care, the hospital deployed DigitalPersona® Pro, resulting in fast, reliable access to Electronic Medical Records (EMR). Jackson Hospital is now able to give physicians and ancillary staff a secure way of accessing patient records, protecting data and improving compliance with the Health Information Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act mandates.

NEEDS

- Fast, secure access to electronic medical records.
- Central management.
- Compliance with HIPAA and HITECH.

DIGITALPERSONA PRODUCTS

DigitalPersona® Pro
U.are.U® Fingerprint Keyboards

"DigitalPersona Pro has substantially decreased the number of forgotten password calls to our help desk."

Richard Caldwell
VP of Support Services
Jackson Hospital

Security Challenge

Physicians must repeatedly log in to Jackson Hospital's EMR as they move from patient to patient. They do not have time to go through a lengthy log in process, yet access must be secure due to strict HIPAA and HITECH regulations.

Jackson Hospital needed a solution that would meet these mandates, while providing a fast and convenient method for physicians and ancillary staff to access their EMR.

DigitalPersona Endpoint Protection

The single sign-on capabilities of DigitalPersona endpoint protection solutions eliminate the lengthy log in process of typing usernames and passwords when accessing the EMR. Jackson Hospital physicians can now use their fingerprints to securely and easily access patient records.

DigitalPersona Pro provides the IT department with a single control point to centrally manage and enforce authentication and access policies throughout their network.

Benefits

- **Fast, Reliable Access to EMR** - Physicians and staff no longer have to remember and type usernames and passwords.
- **Central Management** - Strong security policies are enforced from a single point.
- **Compliance** - HIPAA and HITECH access control requirements are fulfilled.

The Results

Jackson Hospital has improved patient care response time by eliminating lengthy log in processes. Physicians are able to quickly and securely access the EMR, allowing for more time with patients.

The use of DigitalPersona Pro and fingerprint biometrics assists Jackson Hospital in complying with the strong authentication components of HIPAA and HITECH regulations.

In addition, the number of help desk calls have significantly dropped since physicians do not need to remember usernames and passwords.

"DigitalPersona's strong authentication capabilities provide quick and secure access to patient data while our doctors make their rounds," said Richard Caldwell, vice president of support services at Jackson Hospital. "Our physicians really appreciate the time it saves them."

About DigitalPersona

DigitalPersona is a global provider of authentication and endpoint protection solutions that make security simple, practical and affordable for businesses of all sizes. The company helps enterprises, government agencies, custom application developers and independent software vendors to efficiently address growing security, compliance and fraud-prevention demands. DigitalPersona's award-winning technology is offered by market-leading computer manufacturers and solution providers around the world.

digitalPersona®

DigitalPersona, Inc.
720 Bay Road
Redwood City, CA 94063 USA

Tel: +1 650.474.4000
Fax: +1 650.298.8313
E-Mail: info@digitalpersona.com
Web: www.digitalpersona.com

It's Time for a Check-up

Secure Data and Ensure Compliance
with the trusted expert in data protection.

With data breaches soaring and regulations tightening, now is the time to prepare. Whether sensitive information resides on shared medical devices, desktops, laptops, smartphones or USB drives – CREDANT data protection enables you to easily define and enforce security policies from a central console to help you ensure HITECH & HIPAA compliance.

To learn more about non-compliance, see where your organization may be at risk and learn how to assess it, download The Data Risk Assessment Tool for the healthcare industry at **www.credant.com/healthcare**

CREDANT®
We Protect What Matters

www.credant.com

1–866–CREDANT

DETECT | **PROTECT** | CONTROL | **MANAGE**