Contributing Executives

Chris Brooks
SVP of Technology
WebMD Health Services

Sam Curry
CTO
RSA

James Dzierzanowski
Information Security Officer
Dignity health

Howard E. Haile CISSP, CISA
Chief Information Security Officer
SCL Health System
# Table of Contents

Executive Summary ..............................................................................................................4

Healthcare Security .............................................................................................................5-16

10 Steps to Maintaining Data Privacy in a Changing Mobile World ...................... 6
  Consequences of data breaches ..................................................................................... 6
  Lessons Learned — Getting Back to Basics ................................................................. 7

Best Practices for Security in Healthcare ................................................................. 8
  Basic Network Protection ............................................................................................. 9
  Single Sign-On ............................................................................................................... 10
  Mobile Devices ............................................................................................................. 11
  Business Associates .................................................................................................... 12
  Patient Portals .............................................................................................................. 13
  Health Information Exchange ..................................................................................... 14
  Cloud Security ........................................................................................................... 15

Conclusion ..................................................................................................................... 17
  Action Points .............................................................................................................. 18
  Notes ......................................................................................................................... 19
Executive Summary

Cyber criminals are increasingly targeting the healthcare industry, because medical identity theft is more lucrative than the theft of personal identification information alone. Meanwhile, health care systems are increasingly vulnerable to attack as electronic health records spread, and as the use of web portals for information exchange with patients and providers becomes more common.

Healthcare providers and their business associates must comply with a number of security and privacy regulations, including the federal government’s HIPAA and HITECH Act rules, state privacy regulations, and Joint Commission requirements. But, as the growing number of security breaches in the healthcare industry shows, these regulations are insufficient to ensure the protection of personal health information. To prevent security breaches and ward off cyber criminals, providers and insurance companies must use advanced security techniques.

The purpose of this paper is to explain how healthcare organizations can best protect themselves from the rapidly growing threat of security breaches and medical identity theft. CIOs and security consultants will describe best practices for preventing these incidents. They will also suggest how to deal with the proliferation of electronic data on the web and on mobile devices, which has created many new avenues for cyber attacks and the theft of personal health information.
Healthcare Security

10 Steps to Maintaining Data Privacy in a Changing Mobile World

As more and more health data becomes digitized, cyber criminals are targeting the healthcare industry as never before. The rapid rise of data storage platforms that host large amounts of protected health information (PHI), along with the increasing fluidity and persistence of this data on computers, mobile devices and the Internet, has made health care a ripe target for some of the world’s smartest thieves. According to the Ponemon Institute, which tracks this field, criminal attacks on healthcare systems have doubled since 2010.1

Healthcare organizations need to step up their security game to counter this growing threat. While many hospitals and healthcare systems are doing a fairly good job, others may continue to downplay the security situation, experts say. Today, organizations that fail to protect themselves adequately may be vulnerable to security breaches and medical identity thefts that can result in large fines, lawsuits, and reputational damage.

Recent statistics show just how exposed healthcare providers are. Sixty-one percent of global healthcare organizations have experienced a security-related incident in the form of a security breach, data loss, or unplanned downtime at least once in the past 12 months, according to the EMC Global IT Trust Curve Survey.2 Each year, these incidents cost U.S. hospitals an estimated $1.6 billion, which include incidents such as:

- **Security Breaches:** Nearly one in five (19%) global healthcare organizations has experienced a security breach in the last 12 months at an average cost of $810,189 per incident. Health IT executives say the most common causes for breaches include malware and viruses (58%); outsider attacks (42%); loss/theft of equipment (38%); and user error (35%).

- **Data Loss:** Nearly one in three (28%) global healthcare organizations has experienced data losses in the past 12 months at an average cost of $807,571 per incident. Of those organizations, more than a third (39%) have experienced five or more incidents in the past 12 months. Common causes of data loss include hardware failure (51%); loss of power (49%); and loss of backup power (27%).

Another report, based on government data, highlights these alarming facts about health data security:

- From 2009 through 2013, 29.3 million patient records were compromised in 804 data breaches involving more than 500 records each.
- From 2012 to 2013, the number of records included in these security incidents jumped 138%.
- Theft accounted for 83% of compromised records in 2013.3

The correlation between receiving a data breach notification from a healthcare provider and being a victim of fraud increased from one in nine in 2010 to one in four in 2012.4 And 43% of all reported identity thefts in the U.S. in 2013 were medical identity thefts.5
Healthcare Security

Thieves can use healthcare identity data to gain access to medical services, devices and prescription drugs. They can use physician information to create fake prescriptions and then resell the medicine online. And they can file false claims to insurance companies and government agencies, billing for services that were not rendered.

All of this makes PHI very valuable to thieves. They can resell a stolen credit card on the street for about $1 and personal identification information (PII) for $10-$12. In contrast, patient records can command $50 each on the black market.\(^6\)\(^7\)

A Ponemon Institute report shows how quickly medical identity theft is growing. In 2010, the report indicates, there were 1.42 million victims of this crime in the U.S. The number increased to 1.49 million in 2011 and 1.85 million in 2012.\(^8\)

Three-quarters of survey respondents who were victims of medical identity theft reported they had suffered financial consequences, including lost health insurance, higher insurance premiums, lost time and productivity, lowered credit scores, and legal costs. The out of pocket cost for the average victim in 2012 was $18,660.\(^9\)

Consequences of data breaches

Under the latest HIPAA security regulations, known as the HIPAA Omnibus Final Rule, healthcare organizations are required to protect against reasonably expected threats to the security and privacy of electronic PHI. When these rules went into effect in March 2013, the penalties for noncompliance increased to a maximum of $1.5 million per violation.\(^10\) Many states also have privacy laws that specify civil and sometimes criminal penalties for unauthorized disclosures of PHI.\(^11\) And the Joint Commission, which accredits healthcare organizations, requires them to use information systems that provide a high level of security and privacy protection.\(^12\)

Several providers have been sued over their security breaches.\(^13\)\(^-\)\(^14\) Institutions that have exposed thousands of their patients to medical identity theft must also contend with the economic fallout of a diminished reputation.

A recent report showed that a fairly small percentage of data security breaches involved EHRs.\(^15\) But the rapid increase in EHR adoption has led to the mass digitization of healthcare data. With the majority of hospitals and physicians now using EHRs, PHI is more liquid and accessible, and therefore more vulnerable to theft, than bulky paper records in file rooms ever were.

Meanwhile, the federal government has been promoting the exchange of health information among providers. Stage 2 of the Meaningful Use EHR incentive program, for example, requires eligible hospitals and eligible professionals to exchange data online with unrelated providers at transitions of care such as referrals and hospital discharges.\(^16\) The mechanisms to do this include private and community health information exchanges, which present new opportunities for PHI to be lost or stolen.
Healthcare Security

Meaningful Use stage 2 also requires eligible providers to share health records electronically with patients. Most hospitals and practices plan to provide these records on patient portals attached to their EHRs.\(^\text{17}\) While such portals have been around for years, a small minority of hospitals and doctors have used them until now. The security issues presented by patient portals are just starting to be explored, but it’s already clear that portals connecting EHRs to the public Internet create new types of vulnerabilities.

Last but not least, physicians and nurses are increasingly using mobile devices in their clinical work. Many clinicians bring their personal smartphones and tablets to the office and the hospital. These devices present a host of security problems that healthcare organizations are grappling with in a variety of ways.

Lessons Learned — Getting Back to Basics

Faced with these complex threats and the financial consequences of breaches, the healthcare industry is starting to learn lessons from other highly targeted verticals such as the financial industry; in fact, that’s where some institutions’ chief information security officers are coming from.

Nevertheless, many hospitals are just starting to recognize the need for rigorous security policies and effective technological defenses. In a recent InformationWeek article, security consultant Kate Borten states:

From what I see, security savvy [healthcare] organizations are in the minority. Too many organizations’ infosec programs are still very immature. The glaring signs are: 1) lack of internal security expertise; and 2) insufficient resources to carry out security functions.\(^\text{18}\)

Only a small percentage of hospitals have chief information security officers (CISOs) who are dedicated to security, she notes. Too often, overburdened CIOs are given the HIPAA-mandated title of information security officer but have no time to perform the work. That’s one reason why basic security procedures may not be followed. As a result, she says, “lost and stolen laptops, hard drives, USB drives, and the like with unencrypted patient information are the biggest sources of breaches.”

Howard Haile, chief information security officer at SCL Health System in Denver, agrees that having an executive in his role is critical to safeguarding patient data.

“"In the past, healthcare didn’t put a high priority on security. Although we had HIPAA for many years, there weren’t any sanctions around unlawful disclosure of PHI. It was something you needed to do, but if you didn’t do it, there weren’t any consequences around it. Now there are not only sanctions from unlawful disclosure, but there are also reputational consequences that go with it that healthcare is starting to recognize. So having somebody dedicated to that role is crucial."

Only a small percentage of hospitals have chief information security officers (CISOs) who are dedicated to security, she notes. Too often, overburdened CIOs are given the HIPAA-mandated title of information security officer but have no time to perform the work. That’s one reason why basic security procedures may not be followed. As a result, she says, “lost and stolen laptops, hard drives, USB drives, and the like with unencrypted patient information are the biggest sources of breaches.”
Healthcare Security

Chris Brooks, senior vice president of technology for WebMD Health Services, which provides health and wellness programs to health insurers and employers, says that healthcare providers should be concerned not only about the consequences of security breaches, but also about the increasing interest of criminals in healthcare. While cyber-thieves still regard banks as their most lucrative target, he says, “I’m a bit concerned when the spotlight turns to healthcare information, and the syndicates begin to target this world a bit more. I think we’ve had a pass for a while. Most of the breaches you see in healthcare are human error and lost laptops and so on. But we’re concerned that that’s going to change in the near future, and it’s going to require more scrutiny and protection.”

This paper shows how healthcare organizations can protect themselves from security breaches and data losses. In addition, we address the issues created by the fluidity and persistence of electronic data on portals, mobile devices, and the cloud. Knowing how to secure data in this chaotic, quickly changing environment is critical to success in the never-ending war against cyber criminals.

Best Practices for Security in Healthcare

Our contributors represent organizations that have adopted advanced techniques for protecting their data. But they all admit that there are limits to what those methods can do.

For example, Haile points out that there’s no way to prevent laptops and other mobile devices from getting lost or stolen. SCL Health System—which includes the former Exempla and Sisters of Charity systems—has a policy that advises users to keep devices with them at all times, “but they still leave it in the car and it gets stolen,” he says. “Policy is not a security control.” The important thing is to make sure that any patient data on the device is encrypted, he adds.

Another key insight we gleaned from our contributors is that healthcare organizations need to strike the right balance between robust security and ensuring that clinicians have the access to data they need to do their jobs in a timely manner. In healthcare, finding this balance can literally save lives.

“One of the biggest challenges/opportunities for security is how to make it less intrusive while strengthening it at the same time,” notes Sam Curry, chief technology officer of RSA, the security division of EMC. “The less interruptions for the people who deliver the medical service, the better the quality of that service and the more reliable and predictable it will be.”

Haile agrees, but adds that this is a challenging goal. “In any organization, you have to balance security with operations. It isn’t security driving operations; operations drive security, and security should be able to live in harmony with those operations. We should allow our physicians to be able to do their work in a security-rich environment, and I believe that that’s what we do.”
Healthcare Security

With these considerations in mind, here are some of the best practices that our experts recommend in specific areas of security.

Basic Network Protection

Although the protection of PHI is the number one priority of healthcare organizations, they must also be concerned about the potential theft of personal identity information (PII) and credit card numbers. So security staff must use administrative and technical controls to protect all personally identifiable data, whether or not it is healthcare-related. And if they take credit cards, they must also comply with PCI security standards.

The first area to consider is the integrity of the information network in the hospital, practice, or healthcare system. Besides protecting computer servers with firewalls and other techniques, Haile suggests restricting the administrative rights of users based on their roles, “so if something does get stolen, it can’t proliferate. You also do a lot of end-user training to recognize targeted phishing attacks. You do internal filtering [of malicious e-mails] to make sure you protect yourself.”

It is imperative to understand the data flows on your network, he adds. That requires the use of analytics to understand the “context” of how data is being accessed. “Does it make sense that this user is accessing the data, and this user is sharing files? Did this user suddenly get permissions elevated? Those are classic signs of intrusions.”

James Dzierzanowski, senior security director and ISO for Dignity Health, a big hospital chain based in San Francisco, says this organization uses standard corporate detection and prevention techniques. These include continuous security monitoring, intrusion detection system audits and internal incident management.

Our experts disagree on the value of antivirus software. Haile says antivirus is “basically unusable now,” whereas Dzierzanowski views it as a tool that still can be used to scan mobile devices. There have been problems with antivirus in companies that have been breached, he says, “so you have to be vigilant.” Nevertheless, he adds, “malware is an active way to get into the network, so it’s an ongoing threat.”

WebMD still uses antivirus software on its servers, but Brooks admits that it can be circumvented. “I’ve had antivirus programs that had flaws that led to performance and availability concerns,” he points out. “Whether you’re going to use them or not, if you’re relying on those as your primary means [of defense against malware], you’re asking for trouble.”

Another basic tool that some healthcare providers overlook is encryption. Besides encrypting data at rest on servers, organizations should also encrypt PHI residing on client computers and mobile devices. However, Haile observes, it’s difficult to encrypt data when it’s in transit from one device to another in the internal network.
Healthcare Security

“Usually, your data on the internal network is trusted,” he says. “It’s when you flow outside your egress point that it’s problematic. If it’s PHI or PII, you have to encrypt outbound data at the egress point.”

Business associate agreements require outside entities to take responsibility for protecting the PHI they receive from healthcare organizations. But providers must still share liability for security breaches with their business associates.

Single Sign-On

Physicians hate to waste time entering logins and passwords, so many organizations let them access a number of applications with a single sign-on. While this is good for a hospital’s relations with its physicians, it can create security issues by allowing an unauthorized user to access PHI in multiple locations.

SCL gives its physicians and nurses single-sign-on access to clinical applications. Once they log on at a particular workstation, they can use their security badge to return to their session at other workstations in a “tap and go” process. They must be re-authenticated every six hours, or roughly twice in each hospital shift. But the single sign-on enables doctors to see two or three extra patients a day, Haile notes.

At Dignity Health, single sign-on is “vertically targeted,” Dzierzanowski says. The IT department divides network users into different groups, including physicians, nurses, administrators, other employees, and contractors. Each group has single-sign-on access just to the applications they need to do their job. Physicians, for example, have access to all clinical applications, while coders have access to both the EHR and financial programs.

Dignity requires strong passwords, which are 15 characters long for system-level access. Passwords remain active in memory during a clinical session, but they don’t persist in the system. “They don’t reside in temporary memory so somebody can do a RAM scrape,” Dzierzanowski notes.

Users are urged to log off when they leave their workstations; if they don’t, the desktop computer times out. Like SCL, Dignity uses a “tap and go” system with security badges so clinicians don’t have to log back on at their next workstation. Alternatively, they can take laptops with them or have an assistant follow them with a computer cart.
Healthcare Security

Mobile Devices

Four of five physicians said they used mobile devices such as smartphones and iPads in their clinical work in 2011; a year later, nearly two-thirds of doctors were using computer tablets at work, and the percentage has undoubtedly risen since then. It’s too expensive to give every doctor a hospital-owned tablet, which they might not use, anyway. So healthcare CIOs and security executives are faced with the daunting challenge of securing their systems while providing network access to physicians on their personal mobile devices.

If hospitals are not prepared for this bring-your-own-device (BYOD) trend, Curry suggests, they should prevent doctors from accessing information networks on their smartphones and tablets. “But it’s like trying to hold back the ocean,” he says. “Any hospital that hasn’t started to think this through needs to start.”

Among the issues they need to consider, he says, are these:

- How do people on the network interact with the outside world? They shouldn’t be sending PHI to unauthorized parties or personal email from the network.
- Personal devices may carry programs that could compromise the network. Angry Birds could be hiding malware, for instance.
- If PHI is stored on a device, it could persist for a long time—perhaps after the user has authorization to view it or share it with others.

Dignity Health generally doesn’t provide mobile devices to physicians, but some departments do in a few Dignity hospitals, Dzierzanowski says. Therefore, the IT staff must support both managed and personal devices.

Physician leaders and supervisors throughout the healthcare system give each physician or employee authorization to connect their device to the network. But first, users must install a mobile device management (MDM) program on the device.

Dignity’s BYOD policy does not allow any PHI to be stored on a mobile device, and it requires encryption of data in transit. To protect the network, the solutions scan inbound traffic and attachments, and Dignity supports only iOS, Android and Windows devices above certain version levels.

SCL Health System takes a more elaborate approach to BYOD. Like Dignity Health, SCL tries to prevent users from storing PHI on personal devices. However, it’s sometimes unavoidable because physicians who have “pull” with the administration can get permission, notes Haile.
The only mobile devices that have direct network access are those owned and managed by SCL. Personal devices are excluded, but clinicians can use them to access the network through a Citrix session on a public website. Using these “Citrix-driven virtual desktops,” SCL controls everything on the back end, and no data can be downloaded to mobile devices.

“In the future, physicians will have a Citrix Receiver on their personal device,” Haile says. “They’ll click the Citrix Receiver and connect in that way so they won’t have to go in through a web link.”

Texting among clinicians is another rapidly evolving challenge in hospitals. According to Haile, most of the existing security options are “terrible.” SCL will probably use the texting solution of the same vendor that provides the organization with its single-sign-on technology, he says.

WebMD provides its customers with the ability to text members or employees in its wellness programs, but it advises them not to send any PHI in these short messages. Instead, the texts may remind recipients that a health coaching call is scheduled in a few minutes, or prompt them about their diet and exercise goals, Brooks says.

Business Associates

The HIPAA Omnibus Final Rule makes business associates as liable for data security breaches as HIPAA-covered entities are. The rule did not apply to business associates until September 2013, but the threat of sanctions has already induced many of them to sign business associate agreements (BAAs) with covered entities. This includes cloud vendors, many of whom had earlier been reluctant to sign these pacts. Google is the most recent cloud vendor to fall into line, following companies such as Microsoft and Box.21-22

Business associates were involved in 56% of large-scale breaches (500 or more records) from 2009 to 2012. In 2013, they were implicated in only 10% of breaches, which suggests that they’re paying greater attention to data security. But the number of incidents involving business associates has remained about the same. In addition, BAAs don’t necessarily report all breaches to providers, as they’re legally required to do.23

In 2011, Stanford University Hospital discovered that, a year earlier, a billing contractor had allowed a spreadsheet with health data on 20,000 patients to be posted online. Stanford suspended the contractor and offered free identity theft protection services to the affected patients. But it still suffered a tremendous blow to its reputation as the result of widespread media coverage.24

Providers should insist that business partners that have access to PHI sign BAAs and upgrade their security procedures. Dignity Health does this with business associates who store data in the cloud, and it also requires them to be certified by HITRUST for compliance with the Common Security Framework.
Healthcare Security

Patient Portals

Both patient and physician portals are now being subjected to the same kinds of attacks that cyber-thieves have used to target financial institutions for years. Among these schemes are phishing, Trojans, malware, and drive-by downloads. The rapid proliferation of patient portals opens up vast new opportunities for criminals to steal PHI and PII. Among the security areas that healthcare organizations must address are the identity verification of portal enrollees, login authentication, and the securing of consumer access to portals.

Just as hospitals and practices must balance the need for security against the need to give physicians access to clinical data, patient portals must be secured in a way that doesn’t impede the access of patients to their records or lab results. The goal should be to offer strong security controls in the background while making it relatively easy for consumers to log on and use these portals.

To protect patient data on portals, organizations should create a centralized security service that securely enrolls end users, offers a granular authorization policy to control access, secures credentials, and provides positive, transparent user authentication.

Curry points out that when organizations use patient portals to share data from their EHR, the EHR must be able to confirm the integrity of the portal and ensure the confidentiality of the person asking for their records.

“When people build a system behind portals, they use a generic password, assuming that whoever’s asking for information has the right to do so. So the user contact is lost between the portal and the backend database. You need to architect it to say, ‘I have a third system here that does strong authentication, and I trust its data integrity.’ Even if the portal is compromised, all that somebody can see is that there was a request for information.”

Curry recommends strong authentication of users, including challenge responses. “On the back end of the authentication system, you want a behavioral analysis and an intelligence-driven approach,” he says. That approach allows you to detect the difference between patterns similar to those of past intruders and legitimate users.

WebMD’s business is built around patient portals, so it has had plenty of experience with securing them. “The governing approach for us is always defense in depth,” Brooks says. “Those are layers that involve both technology and organizational and process layers.” The latter is as important as the former, he notes. “Part of my responsibility is that people have an understanding of what their expectations are and how we should behave when we’re handling that information.”
Healthcare Security

In most cases, WebMD uses single sign-on for authentication, delegating the initial authentication to its customers. This single sign-on takes advantage of industry standards like SAML 2.0, Brooks says. In addition, the company enforces some password complexity as well as best practices for session management, session timeout, and failed attempt.

For some clients, WebMD provides an adaptive or behavioral-based authentication model. Under this approach, Brooks points out, WebMD will look at factors such as which computer or mobile device is being used to log on to the portal, the time of day, or the location. “We may do additional challenges if something seems abnormal,” he says.

The limiting factor is always the toleration of complexity. “A big challenge that providers like WebMD face is the balance between the procedures that you have users go through to authenticate while trying to make it straightforward for people to get access to the service,” Brooks says. “It’s that balance between usability and experience and convenience and access. Different customers have different set points for that.”

Health Information Exchange

Health information exchange is growing but has a long way to go in most healthcare organizations. Nevertheless, with the rise of private, community, and regional HIEs, this is an important topic for health information security officers.

A government report identifies 12 “enabling services” for HIE security, including:

- Risk assessment
- Authentication of users
- Credential management
- Access control
- Privilege management
- Collecting and communicating audit trails
- Ensuring document integrity
- Secure communication channel
- Preserving document confidentiality
- De-identification of data used for research purposes
- Non-repudiation of origin
- Managing consent directives

The limiting factor is always the toleration of complexity. “A big challenge that providers like WebMD face is the balance between the procedures that you have users go through to authenticate while trying to make it straightforward for people to get access to the service,” Brooks says. “It’s that balance between usability and experience and convenience and access. Different customers have different set points for that.”
Healthcare Security

Healthcare organizations that operate private HIEs must be cognizant of these elements in securing the movement of data among the various providers who belong to the HIE. Provider organizations should also be concerned about the security practices of public exchanges that either store their data or enable users to view it in its native databases. But if a hospital or practice participates in a public HIE, it can reduce its security exposure by not importing HIE data into its system.

SCL, for example, is engaged in multiple HIEs. Haile says he’s not concerned about the vulnerability of the SCL system, because it is only feeding data to the exchanges, not accepting data back from them. If a clinician wants to look up information on a patient, he or she must go to an HIE portal.

SCL, which has an Epic EHR, also uses that vendor’s HIE to allow data sharing among doctors. Physicians can exchange data with other Epic users, including those in different organizations. “I feel a lot more comfort with that, because we’re giving them just the subset of the data they need,” rather than the entire database, he says.

The Direct Project, a government-endorsed secure messaging protocol, is starting to come into widespread use as a method for clinicians to push messages and attachments to each other. Many physicians will use Direct messaging to meet the Meaningful Use stage 2 information sharing requirement. Healthcare organizations should be aware of the security implications of Direct messaging, which can originate in EHRs.

Direct’s security depends on health information service providers (HISPs) that move the data across the Internet. HISPs affiliated with or owned by the leading EHR vendors have been or are being accredited by DirectTrust, which specifies security requirements for sending and receiving Direct messages across HISPs.

Cloud Security

Many providers are moving data to the cloud or entering into Software as a Service (SaaS) agreements with vendors that serve applications to them and store their data in the cloud. But a HIMSS focus group of senior health IT executives last year said they were more comfortable using a private cloud, where they control the data, than a public cloud. They were also more likely to store administrative data than clinical data in the cloud. And they were concerned about the reluctance of cloud vendors to sign BAAs—although many of them have since then, as mentioned earlier.

If a healthcare organization wants to use a cloud vendor, one legal expert says, it should make sure that the company has a comprehensive set of security procedures. At a minimum, the vendor should have third-party certification from an entity such as Services Organization Control (SOC) 2 or HITRUST Alliance.
Dignity Health doesn’t store anything in the cloud, says Dzierzanowski; but if it did, it would require the vendor to sign a BAA and be certified for HITRUST’s Common Security Framework, which is HIPAA compliant. He adds that he is seeing a trend toward HIPAA-compliant data centers. Dell, for example, has such a data center and also is certified by HITRUST.

SCL is already operating a private cloud that gives physicians anywhere, anytime access to their data. “We’ve been a little quick to jump to areas that we don’t know as much about as we should, because we haven’t had a private cloud type of option available before,” says Haile. “It’s user preference-driven a little faster than we’ve been able to catch up to.”

Nevertheless, with a private cloud, “you have control of the data and know where it is flowing,” he points out. “You can do an MDM solution that allows you to write encrypted containers, and if they leave the organization, you can pull the data back with little effort.”

The public cloud creates other kinds of issues, he says. “For one thing, it’s unclear how users can be authenticated if they’re not going through SCL’s active directory. Some cloud vendors are SAML-compliant to allow single sign-on direct to a cloud provider; most are not. So you have to provision and deprovision providers in and out of the system.”

SCL doesn’t do business with cloud vendors if they don’t sign BAAs, he adds. But signing an agreement is insufficient if they store data offshore, where HIPAA doesn’t apply. So he has to ask them where their servers are located. “We can no longer be indemnified for a breach that happens in, say, India.”

In the long run, Haile says, SCL will probably go to a hybrid model that allows it to control its own data in a public cloud. That will remove the need to invest in backend infrastructure for cloud storage, but will still allow the organization to know where its data is and where it’s going.

Sam Curry of RSA observes, “Everybody wants the security and the risk control that comes from private infrastructure. But they also want the flexibility, speed and scalability of public cloud. So private cloud sounds like a reasonable option.”

RSA, he notes, is working on a security “fabric” for a hybrid cloud. “Some things are allowed to exist in the public cloud, others are kept on a client-server network or a private cloud, but you can manage it as a whole for accessibility and security. That’s the ideal.

“If I were in the healthcare space, I’d be looking seriously at private cloud. The hybrid world is where we’ll probably end up, but private cloud will let them have their cake and eat it too, for the time being.”
Conclusion

Advanced security techniques, coupled with best practices and proven policies, can thwart cyber-criminals in healthcare as they have in other industries. But healthcare organizations must take the threat seriously and devote the necessary resources to security. In addition, they must recognize that their changing environment requires new kinds of security measures. Among the factors that should be taken into account are the fluidity and persistence of electronic data, both within the network and across the Internet; the rapid growth in the use of mobile devices by clinicians; the specialized authentication and access control requirements of patient portals; and the evolving security requirements of data storage in the cloud.

Cyber theft can be mitigated. With some notable exceptions, industries such as financial services, have countered this threat successfully. Healthcare organizations can, too, if they make the requisite effort.
**Action Points**

- **Get security expertise.** Hire a chief information security officer who is dedicated to safeguarding your organization’s data. Asking your CIO to add this burden to his or her extensive portfolio invites trouble, because basic security procedures may be overlooked as a result.

- **Strike the right balance between security and accessibility.** While data security is very important, security procedures cannot be allowed to get in the way of clinicians accessing the data they need to do their work.

- **Role-based security.** Restrict the access of individuals, based on their organizational role, to prevent breaches from spreading to the most sensitive and important data.

- **Implement data controls.** Identify the most critical and sensitive information and put data protection controls around that. Depending on the type of information, various security methods can be used, including encryption or tokenization.

- **Use caution with single sign on.** Single sign on poses security threats, but clinicians demand it. To minimize the risk, program workstations to time out and log off automatically. A role-based security approach can be used to restrict access to only those applications a user needs.

- **Address the use of mobile devices.** Organizations that allow BYOD must have policies to prevent mobile devices from endangering network security. They should also prohibit storage of PHI on these devices. Texting requires a security solution, as well.

- **Get business associate agreements.** All outside partners and service providers, including cloud storage providers, should sign BAAs acknowledging their responsibility to protect PHI. You should also require business associates to upgrade their security procedures.

- **Secure patient portals.** Verify the identities of portal enrollees and adopt stringent authentication processes, but don’t make it too hard for patients to log on to portals. Use behavioral and contextual approaches to detect patterns of intruders.

- **Reduce HIE exposure.** Be aware of the security practices of public health information exchanges. If you participate in one, you can reduce your security risk by not importing HIE data into your system.

- **Choose your cloud provider and cloud type carefully.** A cloud service provider should sign a BAA and be HIPAA compliant. Healthcare providers might find the public cloud enticing because of cost efficiencies, but a hybrid cloud might be preferable because it allows them to control their data.
Notes

8. “The Growing Threat of Medical Identity Fraud,”
9. Ibid.
15. “Breach Report 2013: Protected Health Information (PHI)”