Survey Says: Healthcare Leaders Ready to Focus on Information Security
Executive Summary

The passage of the HITECH Act and the push for adoption of Electronic Health Records (EHRs) is creating unprecedented amounts of health information in digital form. While EHRs confer many advantages for both patients and providers, it also generates risk that must be managed effectively. Simultaneously, healthcare staffs are increasingly demanding the ability for universal connectivity and seamless usage of smartphones and tablets. The convergence of these factors has led to more breaches in recent months, many of which affect many individuals in a single incident. Recent legislation has made the consequences of such breaches disastrous.

A new survey of more than 500 healthcare executives shows that organizations are ready to take action. They are appointing chief security officers and pouring more money into information security. By conducting a comprehensive risk assessment and implementing a continuous monitoring strategy, healthcare providers can reduce inherent risks and mitigate the unique challenges they face.

Introduction: The Rising Imperative for Information Security

In Denmark, nearly half of hospitals and almost all primary care physicians use electronic health records (EHRs).\(^1\) Contrast this to the United States, where the adoption rate of electronic records is only about 10 percent. In Denmark, prescriptions are paperless – they are entered electronically.

In some cases, telemedicine affords patients the ability to receive care from their own home, or wherever they may be. Webcams and monitoring devices connected to the patient’s home computer or notebook allow healthcare providers to diagnose and treat these patients remotely. It has taken more than 10 years of experimentation to reach this level of technology integration in Denmark, whereas this journey is just now beginning in the United States. But as Denmark has demonstrated, the benefits of EHR adoption are clear: savings of millions of dollars and vast amounts of time from relief of administrative work.

In playing this game of “catch-up,” the incentives for the United States to rapidly adopt EHR are in place, as are disincentives for losing sight of data security in the process. In fact, the American Recovery and Reinvestment Act of 2009 (ARRA) has breathed unprecedented life into the quest for electronic information, with providers eligible to receive up to $27 billion overall in incentive funds for the “Meaningful Use” of EHRs.\(^2\) In addition to the incentives, healthcare providers also could face reductions in Medicare reimbursement if they do not comply with the legislation’s Meaningful Use standards by 2015 (Figure 1). As a result, EHRs are expected to quickly become the overwhelming norm in the industry, after languishing as more of a dream than a reality for many years. U.S. hospital spending on information technology is predicted to reach $6.8 billion by 2014.\(^3\)

The legislation is not only encouraging the use of more electronic data – it is also expected to result in the digital exchange of information among various providers such as hospitals, clinics, labs and government agencies. Already, more than 67 public health information exchanges (HIEs) and 161 private HIEs have been formed around the country – and these organizations are expected to continue to expand in the future.\(^4\) Future initiatives such as Accountable Care Organizations (ACOs), will accelerate this trend and the demands for seamless connectivity.

---


\(^3\) Health Data Management magazine, “Hospital I.T. Spending Surge Predicted,” June 2009.

\(^4\) http://www.informationweek.com/news/healthcare/interoperability/231700227
Figure 1: Meaningful Use as it Relates to HIPAA

However, a healthy dose of scrutiny over security is required to make the dream of effective EHR a reality. Certainly, it is not surprising to find that information security has become a concern, considering how the industry is moving at a rapid clip toward an electronic future. More data is being stored and transferred in electronic formats, more users are using mobile devices to access this information, and transparency into data security is growing, as the government has mandated that providers report data breaches.

The proliferation of mobile devices in the healthcare environment also is prompting leaders to consider health information security concerns. 72 percent of U.S. physicians now use smartphones, up from just 30 percent of physicians in 2001. In addition, some 39 percent of Chief Medical Information Officers have rolled out mobile computers or handhelds at their facilities, and 86 percent of physicians express that their top interest in mobile technology is for accessing electronic medical records.

In addition, healthcare IT administrators are now faced with physicians’ and other clinicians’ requests to use their own personal devices, such as iPads and iPhones, to access patient information from anywhere, at any time. With these mobile devices, clinicians are able to make faster decisions for their patients.

6 http://mobihealthnews.com/7985/cmios-39-percent-have-installed-mobile-devices/
SecureWorks
Healthcare Leaders Ready to Focus on Information Security

patients, improving their overall workflow and patient outcomes. This technology, however, is not without its risks; and just as it offers faster access to information, such technology can also introduce new ways to compromise information.

Indeed, with more electronic data and increased mobility, healthcare organizations are dealing with a growing laundry list of security concerns such as:

- A proliferation of operating systems to secure, as staff members seek to use their own devices to access data
- Data loss emanating from lost or stolen laptops, USB drives, or other removable media
- Authorized application users misusing information (e.g. looking at sequential patient records, accessing a greater than average number of records, or blatant misuse of data such as celebrity snooping)
- Insiders accessing data aggregation points such as a network database
- Unauthorized users penetrating the network or perimeter
- Multiple authentication mechanisms (e.g. login) and authentication points during the course of a normal day
- Policy enforcement on mobile end points to control applications and internet access

Exacerbating these concerns, if an organization loses more than 500 records containing electronic protected health information (ePHI) in a single event, they must:

a) Notify HHS no later than 60 days.

b) Notify prominent media outlets in the regions where the patients with breached records live.

Upon notification, HHS will post an entry on their website listing the organization, the breach date, and the number of records breached.8

As of April 2011, more than 260 breaches had been reported since 2009, affecting more than 10 million patients.9 The press has devoured stories of these types of breaches, with articles running in all manner of media from healthcare trade journals to mainstream newspapers.

Here are just a few of the recent high-profile breach cases that have made their way into the public consciousness:

- An identity-theft ring managed to breach emergency room files at Holy Cross Hospital, stealing Social Security numbers and personal details of 1500 patients.10
- A BlackBerry was lost in 2010 from SunBridge Health, containing unencrypted information, and involving names, dates of birth, medical record numbers, dates of service and clinical data of around 1,000 individuals. The data was lost for 6 months before all the damage was recovered.11
- WellPoint paid $100,000 to the state of Indiana over delayed notification about a consumer data breach that affected the records of more than 32,000 people. As part of the penalty, WellPoint will also pay for up to two years of credit monitoring and identity-theft protection for all the state’s consumers affected by the breach, and provide up to $50,000 in reimbursement to any WellPoint consumers who suffer an identity-theft loss because of the breach.12

The fact that healthcare data is increasingly attractive to criminals simply heightens the breach

---

8http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
9http://www.eweek.com/c/a/Health-Care-IT/Health-Care-Data-Breaches-Affect-10-Million-Patients-Since-Fall-2009-809191/
10www.phiprivacy.net: “Holy Cross Hospital Notifies Emergency Room Patients of Possible Data Breach,” November 2010
11http://www.phiprivacy.net/?s=sunbridge&amp;x=16&amp;y=3
SecureWorks
Healthcare Leaders Ready to Focus on Information Security

commits and strongly indicates that breaches could continue to proliferate. According to a new report from RSA, a Bedford, Massachusetts-based supplier of risk and compliance solutions, with the pervasiveness of electronic information, healthcare organizations are becoming more attractive to cyber-criminals. Indeed, the street value of a medical record stands at $50 due partly to the ability of criminals to file false claims, whereas the value of a Social Security number alone is just $1.13

Information Security Trends

Dell SecureWorks agrees that security is a critical concern in healthcare. A recent Dell survey of 593 executives representing various provider organizations revealed that the top concerns of executives are increasing budgets to incorporate higher security needs, a lack of resources to tackle security, and mobile device threats.

Approximately 44 percent of the surveyed executives expected information security budgets to increase during the next three years, while only 2 percent expected budgets to decrease. A little more than a third of the individuals surveyed were unsure which direction their IT security spending budgets are heading, and the remaining 21 percent expressed that budgets were expected to remain flat. Taken together, these figures lead to the conclusion that direction and prioritization is needed for many healthcare providers, and that large populations of providers already recognize that increased investments are necessary to sustain or improve the integrity of their security posture.

Going Mobile

With the advancement of electronic data and mobile devices, it is not surprising that protecting mobile data is now a top concern, with 55 percent of the polled health leaders identifying un-encrypted patient data on laptops, smart phones, tablets and other devices as their most pressing health information technology security vulnerability concern. And justifiably so: between August 2009 and December 2010, 65 percent of the breaches that were reported to HHS were the result of lost or stolen mobile devices and laptops.14

Paradoxes in Information Security Practices

In essence, the results make it reasonable to infer that healthcare leaders are making information security decisions under the following paradigms:

Compliance-driven information security decisions. More than 70 percent of health leaders report that compliance with government regulations is their primary motivator for information security purchases. Under this scenario, it is likely that healthcare personnel are persuading leaders to make investments in security technologies and programs in an effort to meet specific requirements of various regulations. Broader security programs are much more nebulous and therefore, success is much more difficult to define.

Reactionary decision-making. With technology constantly changing, and the media pouring out stories of data breaches, healthcare leaders are apt to respond to the “fear” of the moment. For example, if a large data breach tied to the use of laptop computers is reported, leaders might zero in specifically on security solutions designed to keep data safe on these devices. Under this scenario, healthcare organizations are likely to make “knee-jerk” reactions, investing in security technologies or programs that address the security “issue of the day.” As such, organizations are likely to make investments in an effort to avert crises. These investments, however, are unlikely to produce

SecureWorks Healthcare Leaders Ready to Focus on Information Security

effective long-term information security programs that support organizational goals.

The Need for a New Information Security Paradigm

To more effectively deal with information security in the information age, healthcare providers need to make it a strategic pursuit. Instead of simply reacting to the call for compliance or the need to prevent or respond to a breach, healthcare leaders should adopt a more holistic approach.

Consider the following example: Hospital leaders decide to expand service lines, offering elective surgeries as a means to bring in additional revenue at higher reimbursement rates. To do so, the leaders need to put together a business strategy that includes planning for new physical space, purchasing new equipment and implementing new information technology.

With this business plan in place, leaders then should conduct a detailed risk assessment to identify any and all security vulnerabilities. This assessment is an on-going process of discovering, correcting and preventing security problems. It can be conducted in three concurrent phases:

- **System Documentation Phase**: Identifies all of the systems that support the business operation.
- **Risk Determination Phase**: Pinpoints relative risk based on likelihood of occurrence and value of target.
- **Safeguard Determination Phase**: Highlights what safeguards can be put in place to mitigate the risks.

A comprehensive program that involves conducting the necessary risk analysis, and having the appropriate people, processes and technology in place for monitoring and reacting to threats and breaches before they affect ePHI can not only save significant time, but significant damage to the organization’s reputation and bottom line.

The primary impetus for starting with a risk assessment as a foundation for IT strategy is to not only help the organization meet compliance requirements such as HIPAA and Meaningful Use, but also to take a substantial step in creating the capability to react to and mitigate the damage from breaches, which are an increasing likelihood with the proliferation of EMR implementations and recent spikes in device usage. Having a comprehensive picture of where data is, how it is used, and who is accessing it can go a long way to maintaining integrity of patient records, preventing negative press, and avoiding substantial fines and penalties. With a “perfect storm” brewing of looming federal audits, penalties under Meaningful Use, and the Breach Notification Rule, a level of federal scrutiny exists that threatens those organizations that have not planned for and understood the security risks they now face. Ultimately, in healthcare information security, the old adage may now be truer than ever: “an ounce of prevention is worth a pound of cure.”

For more information about Dell SecureWorks, visit www.secureworks.com

In fact, a risk assessment and analysis is the primary starting point for securing mobile devices and policies and meeting the Stage I security requirement for Meaningful Use of EHR, which are two of the primary concerns facing healthcare providers today.