



A hefty penalty imposed on CVS Caremark after its breach of HIPAA regulations was just one of several information security-related topics discussed at a recent SC Magazine Health Care Security Roundtable.

The invitation-only event, held during the summer, gathered together various senior IT professionals to share their thoughts, war stories and advice about some of the information security threats and compliance demands the health care market is facing. Engaging in a half day of discussion and networking, professionals there explored such topics as data theft, regulatory mandates and more.

“There’s no doubt that the U.S. health care system is entirely too fragmented. In order for us to give better care, in order for us to have a health care system that effectively works and that brings down cost, we’re going to need to exchange information via electronic health records (EHRs),” Contino said at the event. “But, the flipside of that is we also need privacy and security protections. Without the security framework we’re going to have trouble.”

The *Health Information Technology for Economic and Clinical Health Act*, or *HITECH Act*, which was passed as part of the *American Recovery and Reinvestment Act of 2009 (ARRA)*, is particularly interesting given that its impacts already are being felt in the industry as a result of the CVS case, said Contino. Providing the teeth that *HIPAA* essentially has been missing since its inception, *HITECH* “is now enhancing the requirements and expanding the scope of *HIPAA* by making [business associates] responsible at the same level of a covered entity.” It also creates a federal breach notification law that has both criminal and civil penalties that are now starting to be prosecuted, he said.

Enter the multimillion dollar fine that CVS Caremark had to pay. As well, the Federal Trade Commission (FTC) listed a bevy of requirements that the company would be obliged to fulfill, including the implementation of an information security program, with proof of its effectiveness being tested by a third party every other year for 20 years. Too, the company

is tasked with designating an employee to create a written program outlining the actions it will take to protect information collected from consumers.

This and many other exposures that have been covered in media outlets is no surprise to many experts.

“Health care management has been far more likely to respond to regulators and industry groups than decide on its own to spend on modern security controls,” said Henry. “Patient data was left at higher levels of risk for loss and breach than in more tightly regulated and consumer-driven industries.”

Aggregate EHRs

Regulatory mandates and other industry-wide requirements, though, are just one small part of a larger security problem that health care organizations must solve.

“In my observation, hospitals seem to be behind the technology curve. In general, when you compare the health care sector to [others], we’re...about 10 years behind the curve and that’s probably being conservative,” Contino said.

This lag is due to several factors, according to many of the industry professionals at the SC Magazine Roundtable. One of the major contributors is that health care data – and how it is collected, stored and shared – is handled much differently than in most other sectors. Whereas other records can be dealt with discretely during some sort of business transaction, the sum of one’s health care history is typically required during a medical occurrence.

“The doctor needs to see a complete set of data in context about a patient,” said Contino. “We have a broader, deeper set of information that needs to be exchanged in health care. A bank can put security parameters around a transaction very nicely, but in health care we can’t do the same kind of incapsulation. So the security controls are different.”

LABOR PAINS

As an increasing number of patient medical records go digital, health care security pros face some trying times, reports [Illena Armstrong](#).

For years, the bark of the *Health Insurance Portability and Accountability Act (HIPAA)* has been loud and clear: Health care entities will be punished for exposing patients’ electronic protected health information (EPHI). But, when the final rule adopting *HIPAA* security standards finally took effect in 2005, its bite largely was that of a toothless, old dog.

Enforcement was all but absent and too few health care organizations were called to task for any signs of impro-

priety. Yet, there were plenty of them who were far from meeting the security expectations *HIPAA* set. According to Reed Henry, senior VP of marketing for security and compliance management vendor ArcSight, compliance with the health care mandate was well below 25 percent in 2005. At the time, corporate leaders had little desire to be told how to run their businesses and also voiced complaints about *HIPAA* security requirements being too vague and difficult to implement.

“Fast forward to today: High profile breaches, clear law enforcement penalties, greater public awareness of identity theft and much clearer regulations by individual state regulators [all] have changed the formula and breach/risk economics,” explained Henry.

Sponsored by
ArcSight

It also helps that *HIPAA* has the weight of the Obama administration behind it. Just one day after the president signed the \$787 billion economic stimulus package earlier this year, government agencies announced that CVS Caremark, the parent company of the largest pharmacy chain in the United States, would be required to pay a \$2.25 million fine for possibly exposing the health care records of millions of its customers.

The hefty penalty and other legal obligations that CVS Caremark likely will be fulfilling for some time is the culmination of just one of the recent data exposure incidents in the health care space that should be putting information security officers and their bosses on notice, according to Paul Contino, VP of information technology at Mount Sinai Medical Center. Contino spoke about this and other information security-related topics when he kicked off a recent SC Magazine Health Care Security Roundtable in New York, which was sponsored by ArcSight.

According to Lou De Frisco, an information technology and security consultant in New York, who has overseen security for the likes of Pfizer, the issue of being able to control and yet share summative medical information is the core problem for health care organizations.

“To be able to do a proper job of health care for a patient, you have to have more of that information aggregated [in one place and that] is what I saw as something of a challenge,” he said at the event.

And, while proper balance of controls with access is a principle all industries must adopt, this requirement to have cumulative data at the ready makes the execution of such a core security tenet that much more difficult.

Then and now

This problem is further compounded by undersized IT security budgets, which are atypical when compared to other industries, said Contino. The financial services vertical allocates about eight to 12 percent of revenues for IT, while high-tech firms spend 20 to 30 percent on technology, he said. Overall IT budgets for health care, on the other hand, are somewhere between three and five percent of revenues, making the amount of money focused on information security miniscule – even though budgets have increased over the years.

“We’re implementing more electronic systems and we’re improving more applications, but, oftentimes, justifying the additional budget for security infrastructure just isn’t there because it’s not forward-facing. It’s not something your CEO or CFO can really get their hands around,” explained Contino. “We’re not keeping up with security in terms of the risks and vulnerabilities that come with having new electronic data sources and new elective systems on the network.”

And a review of the Identity Theft Resource Center’s breach statistics for this year reveals just how little the health care vertical is focused on information security, added Contino. Taking into account a total of some 8.6 million



“Health care has always been an area where dollars and cents are important,” said Larry Maggiotto, CIO of New Island Hospital.

records (13 million at time of publication) being exposed, Contino estimated that approximately 70 percent of those records came out of the health care space. When contrasting this with the government and military verticals, where more breaches have occurred, the level of exposed records was considerably less.

“So, looking at security controls that have been put in place, the military and government have much higher integrity,” said Contino. “Health care tends to be a soft target and that’s going to become an even bigger challenge with greater electronic data systems – EMRs,

PHRs [personal health records], all the hot buttons in health care right now.”

Economic environment

Current economic gloom has wrecked already low budgets in the health care space even more. Attendees at the health care roundtable noted any number of capital IT security projects being cut. As a result, many organizations are finding ways to address security risks piecemeal until budgets loosen.

On the flipside, however, information security has gained some wins here and there as a direct result of a bad economy,

but executive leaders could be prosecuted personally, he said. Secondly, states’ attorney general offices are now the enforcement agents of the *Health Insurance Portability and Accountability Act (HIPAA)* security requirements.

“Because these are political offices they have a personal incentive to put you on the front page – it makes them look good. So now it’s not some anonymous bureaucrat sitting in the Office of Civil Rights [which was tasked with enforcement of *HIPAA*] thinking about whether or not to bring a *HIPAA* violation. There could be a state attorney general looking to get re-elected,” Smith explained. Both addendums, he added, likely will prove “good motivators.”

OBAMA SUPPORT: More effects felt

Debates over budget, support and resources for information security may fade a bit more because of the passage of President Obama’s stimulus bill in February.

According to Larry Smith, senior adviser of information security strategy and policy management at Anthem Blue Cross & Blue Shield, there are two items in the bill that could help strengthen support by corporate leaders for critical information security projects and additional spend.

First, the bill brings with it the application of criminal penalties for data breaches. That is, not only would an organization pay a fine,

said Ken Frantz, principal of Ken Frantz Professional Services and former CISO at Children’s Hospital of Philadelphia.

“There has been some benefit because some of the projects that would be more remote access and more technology, they’ve been cancelled as well, so some of the risks go away. And because these new technologies, applications and projects are on hold, the security of an organization can mature a bit more in the meantime.”

Still, health care traditionally has been a difficult space to navigate when trying to grab funding for information security projects, said Larry Maggiotto, CIO of New Island Hospital in Bethpage, N.Y.

“Health care has always been an area where dollars and cents are important. Do I spend \$100,000 on your system or fix the operating room? It’s always tough to argue against that,” he said.

That’s why IT pros must be aggressive, but in a pleasant way, he added. “One of my old bosses used to say, ‘I can’t afford all the money you’re saving me.’ But that’s what it comes down to. It becomes part of what the CIO role is and what we need to do,” Maggiotto said. “You’ve got to start building consensus with the other senior managers. If you believe in this particular project and you believe security is important, you have to keep fighting for it.”

Beyond the C-suite

Persistence is key when attempting to overcome either indifference or a lack of understanding about IT from health care personnel, as well. While any robust risk management and information security plan hinges on people, process and technology, often the most difficult of these is getting the backing of employees, said De Frisco.

“They understand the need for security. They just don’t want it impacting their productivity,” he said.

Another issue is that some staff may have unrealistic views of what IT departments can achieve for them.

“I call it the Hollywood reality. You’ve got shows on TV or movies where somebody is on a PDA downloading stuff from satellites and in two seconds is looking at fingerprints. OK, when can I have that? If *CSI* can do it, why can’t we do it? But it doesn’t work like that,” said Maggiotto. “Usually, it’s a patchwork of systems we all have to deal with. Trying to put it all together in some kind of plan is the challenge we’re all faced with, but selling is really the key to its success.”

Selling security, assuring staff

One way to sell security is to reassure staff that controls still will allow ready access

to necessary systems. This means, though, that any information security mechanisms implemented must either be transparent, help to enable the business, or simply avoid slowing workers down. In short, security can’t impact business operations.

The consensus of attendees was that technology and processes can help push security forward, but people play a needed role. So, the development of end-users’ IT knowledge is vital. They must understand the consequences of any actions they take. It’s also imperative that they actively engage in corporate security awareness and training programs.

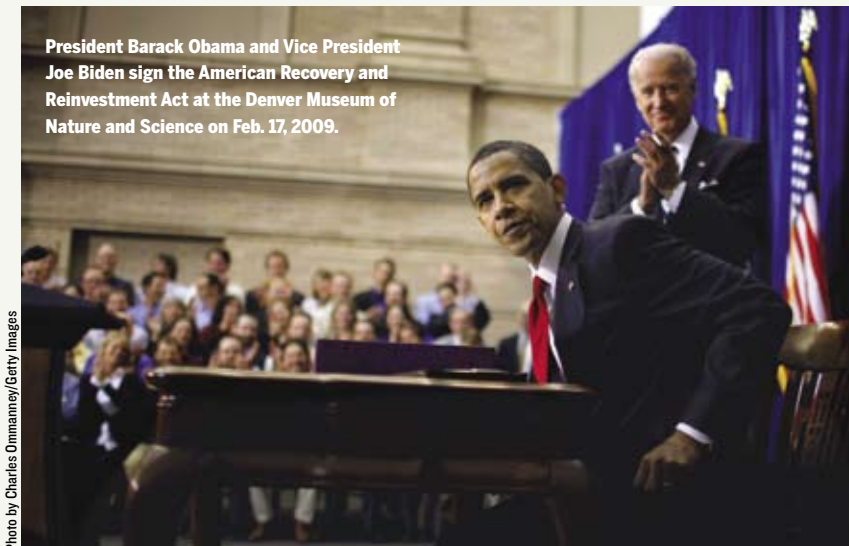
“I think this is somewhat the result of the security norm falling under IT,” said Larry Smith, senior adviser of information security strategy and policy management at Anthem Blue Cross and Blue Shield. “Security is too often focused on tools and technology. One of the problems we’ve had in the health care space is that there hasn’t been enough attention on creating a security mindset in our employee base.”

Accounting for technology

Beyond the establishment of such a mindset, CISOs must consider certain technologies to support the various policies and best practices that they are implementing. Some inevitably will take priority over others during the budgeting cycle.

In particular, solutions that help medical and health care staff do their jobs efficiently and, at the same time, protect patient data, are getting top billing among many organizations right now. So, anything from tokens, single sign-on, identity management tools and others are the solutions supported and deployed. Too, some Roundtable attendees noted that data leakage prevention offerings also have backing and budget. Over and above solutions that may make the IT department’s job easier, the ones that safeguard access to information and help mitigate data exposure seem to be the current tools of choice.

“In health care...the focus is really on enablement. So, when it comes to logs, log management and getting all



President Barack Obama and Vice President Joe Biden sign the American Recovery and Reinvestment Act at the Denver Museum of Nature and Science on Feb. 17, 2009.

Photo by Charles Ommanney/Getty Images

that data correlated – that’s really...for the IT staff...to be information-aware. That has nothing to do with the users, nothing to do with the business,” said Larry Whiteside Jr., CISO, Visiting Nurse Service of New York. “This is the one arena where we really have to focus on enabling our end-users – the nurses, the doctors.”

Nonetheless, most security pros acknowledge the need to understand all that’s happening on their networks. As part of the overall IT governance process, security in all its forms is being accounted for when deploying massive IT systems in health care, such as EpicCare EMR, which is software specifically engineered for the health care

space that provides integrated access for doctors and patients to required data from anywhere, said Frantz.

Still more riddles

Plotting a successful course through budget talks or routing through the complexities of regulatory compliance demands are only some of the areas in which IT security pros need to take the helm. They also must contend with complex systems supported by medical vendors whose products often fail to integrate. Too, they face a lack of standards in the industry to share EHRs among various entities.

“A lot of the vendors in this space have not had a robust tradition and legacy in security,” said Contino, adding that sys-

tems used in this particular sector have been cobbled together by health care professionals or simply have been connected over time as multiple companies have been aggregated or merged.

However they’ve come to exist, the medley of systems on which many large health care organizations have come to rely are filled with security gaps. And medical vendors often are slow to help. They are behind in adopting both security standards and architectures, said Contino, typically because the standards are difficult to implement and there’s really no mandate in place requiring that security be part of their architectures.

Additionally, their solutions, which frequently create the backbone of most

health care organizations’ operations, aren’t interoperable. More problematic: The desire for these vendors to engage in discussions on this subject is low, said Contino. After all, the more interoperable their customers’ systems, the easier it is for them to switch to other vendors.

On top of industry efforts encouraging vendors to address interoperability and security weaknesses in their offerings, pains are being taken to establish standards for information sharing among health care entities. As more and more organizations buy into and implement EHRs, interoperability of this data and the ability to share and access it beyond an organization’s own four walls becomes crucial, said Contino.

One of the first organizations to tackle this issue was Health Level Seven (HL7), a standards development organization founded in 1987. The nonprofit group has been working to create standards and an overarching framework that would, according to its website, enable “the exchange, integration, sharing and retrieval of electronic health information that support clinical practice and the management, delivery and evaluation of health services.” About 500 of its 2,300 members “represent more than 90 percent of the information systems vendors serving health care.”

Meanwhile, the Health Information Trust Alliance (HITRUST), an industry body comprised of vendors, health care companies and others, also released a set of best practices to help organizations move forward with constructing a security framework for their companies. Called the Common Security Framework (CFS), these more prescriptive standards are backed by the likes of Kaiser Permanente, the Children’s Hospital of Philadelphia, and others.

Additional efforts for data exchange also are underway, which do help, said Contino, but much of the work being done in the health care space skip security as part of the frameworks.

“They address messaging, they address data structures, interoperability and



Larry Whiteside Jr., CISO, Visiting Nurse Service of New York, said many executive leaders have little IT security know-how.

ontology of how data gets described between systems,” he noted. “[But] they are not at all security standards.”

Moving forward, then, one of the real needs is to keep in mind security during standards development, he added, especially given the \$19 billion that has been appropriated for medical records to go digital.

“What have we done if we don’t have security? We’ve taken a fragmented paper-based health care system and we’ve created a whole bunch of silos of electronic data that become targets if security’s not there,” he said. “Without a security framework that is adopted by our vendor community, we’re going to wind up having an incredibly high-risk situation for our health care industry.”

No easy fix

Going digital with all medical records could mean huge cost-savings for health care organizations, as well as allow more ready access to massive amounts of data during medical emergencies. Yet, as both government and health care leaders drive the demand to make EHRs happen so that more entities, caregivers and their patients can exchange and access that information as necessary, security and privacy mechanisms become critical. And, with a legion of regulatory mandates affecting health care, so do compliance obligations.

“Behind them all is the same basic set of requirements, which security professionals will be able to decipher and manage just like a doctor can help a patient figure out how to be healthy,” said ArcSight’s Henry. “Staying healthy is like staying secure. Assign responsibility, document goals and principles, [and] then work toward establishing a sustainable process with controls that will detect, prevent and respond to incidents.”

With a robust risk management plan in place based on general best practices, critical data and ultimately the organization can be protected. Today’s signpost for information security leaders is understanding that such planning is a vital component that helps to form the foundation of any business.

“The challenge in securing health care data is that there’s a tremendous dichotomy,” said Contino. “We have on one hand the need to protect the privacy and security of our patients’ records. But on the other hand, we have to be able to completely expose the records and provide timely access to the records for treatment and medical care. And so we have to be able to do both in a way that preserves the security and the integrity of the data, but also does not create impediments for physicians.” ■

A more extensive version of this article is available on www.scmagazineus.com.

SCARE TACTICS: FUD works

Because there still remains a bit of denial among the C-suite about information security needs, IT pros find that calling out their peers’ tribulations still generates executive attention – and budget.

“I think the fear, uncertainty and doubt (FUD) argument is still alive after all these years,” Ken Frantz, principal of Ken Frantz Professional Services and former CISO at Children’s Hospital of Philadelphia, said at the SC Magazine Health Care Security Roundtable. “I used it 15 years ago to sell. It worked then and works now.”

Particularly, as organizations in his sector rely more and more on electronic health records (EHRs) as the foundation of their businesses, FUD likely will have a place for some time. This is because senior-level executives often think that once a costly security project is completed, enough safeguards are in place to protect critical data, said Paul Contino, VP of information technology, Mount Sinai Medical Center. What they fail to fully understand is how quickly networks

change, he added. If, for instance, access rights to the infrastructure are provided to 50 partners after a multimillion dollar project to secure the network is finished, new risks are introduced.

“Unfortunately, they would like to put their heads in the sand and say we’re fine,” he said. “It’s my job to educate.”

Larry Whiteside Jr., CISO, Visiting Nurse Service of New York, agreed that education is critical in the health care space since staff often have little IT security know-how.

“The analogy that I continue to use is that security is sort of like insurance,” he said. “We

all have insurance just in case, because the expense that we would incur if we didn’t have it outweighs the cost of paying for it now.”

Lou De Frisco, an information technology and security consultant in New York, has found that FUD had a major place during a budgetary debate a couple of years ago, “but then [information security] turned more into business value,” he said at the event. Risk management programs today focus more than ever before on compliance, improvement of security postures and tying together all the best practices that support these endeavors to the business. – IA



Photo by Tim Boyle/Getty Images

CVS Caremark is required to pay a \$2.25 million fine for violating HIPAA requirements

COMPLIANCE CONSIDERATIONS FOR HEALTHCARE: Looking Outside for Lessons Within

Healthcare organizations face a daunting task. In addition to transforming their systems and culture from paper-based to electronic records, they have the additional burden of keeping some of the population's most confidential information private – all while devising a way to share information with the doctors and nurses who need it.

A number of industries are a little farther along in this transition to digital records. If we look to those industries, which have been subject to years of regulatory oversight with a clear IT security component, we find a few fundamental lessons to be learned. By keeping these in mind, healthcare security pros can avoid the pitfalls that have plagued other industries.

Consolidate Compliance Efforts

Talk to large banks or global retailers and you'll find they've learned the hard way that defining security policies and compliance programs in a siloed manner comes at a huge long-term cost. There are significant synergies to be had by consolidating compliance efforts across regulations early on. So make sure security policies can be extended to multiple regulations (PCI, SOX, state data breach laws, Red Flags Rule, etc.) and to other types of sensitive data beyond electronic health records.

Don't Forget The Big Picture View

In response to rising threats and growing regulatory pressure, other industries have invested in a slew of security technologies. These investments have provided some protection against specific threats but have not enabled the much needed organization-wide visibility. So take the big picture approach to managing threats and risk and make sure your next security or compliance investment enables greater visibility into a broad range of threats and sources of risk.

Build A Culture Of Security

It might sound clichéd to say that effective security is a function of people, process, and technology, but you'd be surprised how often this is overlooked. Compliance and security projects continue to fail because policies are not formally developed up front or because user awareness and training is not made an integral part of a technology roll-out.

With the recent reinforcement of HIPAA and the growing number of state privacy laws, the healthcare sector has a number of challenges to face. In the scramble to invest in technologies that can help tackle these challenges, it's easy to lose track of the fundamentals. Other industries have been there, and the three obvious but often overlooked considerations described here can help ensure the same mistakes aren't repeated.

Priority Health Proves Compliance, Gains Unprecedented Visibility

Priority Health's Challenge

The need for Priority Health to monitor its networks, servers and applications – and thereby protect itself and its customers from potential threats – has always existed. This need took on greater urgency in the wake of the Health Insurance Portability and Accountability Act (HIPAA) and the organization's own desire to bolster IT security and further secure patient data. However, until Priority Health discovered ArcSight, there was simply no available technology that could completely address their security goals.

The ArcSight Solution

The ArcSight deployment immediately addressed the most serious issues at Priority Health. Whereas security systems once operated in silos without any sharing of information, suddenly data from firewalls, syslogs, IDS and even Web servers was integrated into a single console – providing much needed visibility across the organization.

Just as importantly, ArcSight ESM and ArcSight Logger allow Priority Health to better manage its vulnerability assessment data, and track that data over time. The bottom line is that the organization has become much more adept at managing vulnerabilities and measuring the overall performance of the information security platform.

With ArcSight solutions, potential threats can be quickly contained because the system automatically recognizes unauthorized activity, creates a security incident ticket in real time and immediately notifies the appropriate people of the event.



"Thanks to ArcSight, it became very easy to look at a series of security events – regardless of which device they came from – and see the real scope of the problem and respond appropriately."

- Paul Melson, Manager of Information Security, Priority Health

Impact Highlights:

- Compliance with HIPAA-related requirements, as well as internal security regulations and policies
- Integrates security data from across the organization on a single console providing true visibility into the full-range of security events
- Greatly reduces false positives by filtering down 2.5 million security events to a much more manageable and meaningful number

"...make sure your next security or compliance investment enables greater visibility into a broad range of threats and sources of risk."

Reed Henry, Senior Vice President of Marketing, ArcSight

Mr. Henry is Senior Vice President of Marketing, ArcSight. He holds an MBA from the Stanford University Graduate School of Business, an M.S. in electrical engineering from the California Institute of Technology, and a B.S. in electrical engineering from the University of Washington.

DOWNLOAD NOW

Industry Brief: Healthcare Providers

Industry Brief: Healthcare Payers

White Paper: Healthcare Security Oversight for HIPAA Audit and Compliance

Full Case Study: Priority Health



ArcSight Headquarters: 1-888-415-ARST
© 2009 ArcSight. All rights reserved.

