Healthcare

New law pushes data safeguards forward

ebook

An SC Magazine publication

Sponsored by

HITECH: A new security agenda

A look inside the federal *HITECH* legislation and the changes it is bringing about among Healthcare providers, payers and business associates. Beth Schultz reports.

Privacy and security have been watchwords for the Healthcare industry for ages, it seems, with everybody from the little old lady down the block to the CEO of the sprawling medical facility in the center of town well aware of the ubiquitous *HIPAA* acronym and its meaning.

Patient identities, medical records and other protected health information (PHI) need guarding, and Healthcare organizations have been legally obligated to do so since 1996 when Congress passed the *Health Insurance Portability and Accountability Act* (*HIPAA*). To varying degrees, Healthcare organizations have spent the last 14 years seeking out the right mix of people, processes and technology to get security and privacy squared away. Some give more weight to security and patient privacy risks than others.

At all too many Healthcare institutions, funding projects aimed at ensuring the security and privacy of PHI have taken a second seat to spending initiatives aimed at improving patient care. Truth be told, Healthcare organizations have had nothing to fear. While *HIPAA* got everybody thinking about and moving on securing information assets, it provided virtually no incentive for actually doing so.

Jon Gossels, president of SystemExperts, a network security consulting firm in Sudbury, Mass., even goes as far as saying that many Healthcare organizations made a conscious business decision to ignore *HIPAA* compliance. The low compliance rates, he says, are directly attributable to lax enforcement over the years.

Healthcare organizations certainly didn't have anything forcing their hand, so they did end up viewing *HIPAA* more of a recommendation and guidance than real regulation, agrees Paul Contino, vice president of IT at Mount Sinai Medical Center and Mount Sinai School of Medicine in New York. But that was before the economy hit the skids and President Obama signed into law the *American Recovery and Reinvestment Act of 2009 (ARRA)*, otherwise known as the stimulus act, and penned the *Health Information Technology for Economic and Clinical Health Act*, or *HITECH Act*, into existence last February.

Now, you'd be hard pressed to find a Healthcare organization or any even remotely affiliated business operation that touches patient data that isn't taking the security and privacy of PHI seriously. The stakes have risen.

The carrot and the stick

The Obama administration wants the majority of Healthcare organizations – 90 percent of all clinicians and 70 percent of all hospitals – off of paper and using electronic medical records (EMR) by 2011.

"With *ARRA* came a lot of fanfare with $19 billion of stimulus money designated for pushing forth the EMR agenda in this country," Contino says. But that was tempered, he adds, with the *HITECH* legislation in which, for the first time, the federal government got prescriptive about what was going to be expected for that funding.

"People saw this pot of gold they were going to be able to reach for with EMRs, but, truthfully, at the same time the government started to give *HIPAA* teeth to enforce privacy protections and security,"he says.

ARRA and *HITECH* are both good things, to be sure, Contino adds, but timing is a problem. Healthcare organizations need to show meaningful use of EMRs by 2015 in order to garner money from the stimulus act, he explains. "At the same time, we've got *HITECH* starting to turn some screws on how we can deal with EMRs, and that's going to be a bit of a challenge. While some things in *HITECH* are still being worked out, they

46

states and one territory have notification rules in place

may cause problems with vendors on how to comply, for example, with encryption of medical data," Contino says.

Between the vendor community trying to meet encryption standards and Healthcare organizations adopting EMR, "we may end up with a lot of places that won't be able to implement either in the short term," he adds.

A whipping post

HITECH introduces a number of changes to *HIPAA* requirements and enforcement that do indeed punch up privacy and security regulation for the industry – especially when considered in light of increased EMR use, Healthcare experts widely agree.

> "We're taking a fragmented paper process and moving it forward..."
>
> – Paul Contino, VP of IT, Mount Sinai Medical Center

Among the changes: Healthcare organizations suffering a security breach affecting 500 or more individuals now must not only notify individuals of unauthorized disclosures of their unsecured PHI, but also report said incidents to the U.S. Department of Health and Human Services (HHS) for public notice. As of mid-April, the HHS has posted breach notices from 59 organizations, including several just over that 500 mark and a couple with multiple hundreds of thousands of individuals affected.

The HHS breach report is a list on which no Healthcare organization wants to find its name, says Paul Melson, manager of information security at Priority Health, a health insurance company based in Grand Rapids, Mich. At the least, a marred reputation is hard to clean up in consumers' eyes.

"*HITECH*'s mandatory notification and public notice requirements have been enough to get people to wake up and take notice that the game is changing," Melson says.

And if notifying customers, filing federal reports and publically acknowledging security lapses isn't enough to shake up the industry, the heavy fines – up to $50,000 per incident and $1.5 million annually – now imposable are. The substantial increase in penalties has indeed sent ripples of fear throughout the Healthcare industry, says Chris Apgar, founder of Apgar & Associates, a Healthcare security and privacy consultancy in Portland, Ore.

And *HIPAA*-defined covered entities – health plans, Healthcare clearinghouses as well as Healthcare providers – aren't the only ones fretting. So too are many of their business associates – companies such as insurance firms, benefits managers and payment systems providers that now find themselves under the same *HIPAA* privacy, use, disclosure provisions and security rules as covered entities and, therefore, subject to the same penalties.

Hyland Software, an electronic document and workflow management solutions provider, for example, has been working with its Healthcare customers on addressing the *HITECH* business associate rules in contracts, says Susan deCathelineau, Healthcare solutions manager at the company.

"We've seen changes in how organizations assign a business associate, the agreements we have in place and our partnerships with our customers and other technology vendors. We're now more able to support the privacy of the patient information that could be impacted based on the relationships we have and the work we're doing in supporting and implementing that technology," she says.

Everybody is worried. They've got CVS Caremark on the brain, says Apgar, referring to that company's February 2009 decision to pay $2.25 million to resolve HHS allegations that its pharmacy business violated *HIPAA* regulations by improperly disposing of PHI and risking unauthorized disclosure of that information. On top of that, business associates are concerned that clients will dump them if they do not demonstrate that they have appropriate security and privacy policies and procedures in place, Apgar says.

59

organizations have been breached and notice posted with the HHS as of mid-April

"It's interesting that the 'Oh my gosh, I need to comply' panic is occurring most not with the covered entities, but the business associates – even though they were supposed to be complying all along via contract," he adds. "Now that they're subject to the civil and criminal penalties, there's an added incentive."

When it comes from the business associate perspective, Priority Health's Melson agrees. "You've got far more skin in the game now with *HITECH* than you did with *HIPAA*."

Stacking the decks

HHS also has new clout, notes Scott Heffner, network operations manager at Wentworth-Douglass Hospital (WDH), a small Healthcare provider in Dover, N.H.

Not only does *HITECH* lay out an increase in civil monetary penalties, but it also calls for distribution of collected fines to the HHS's enforcement arm, the Office of Civil Rights. Heffner says he considers this new policy the biggest signal that the government just got super serious about enforcement.

"If you want to get someone motivated to really dig to find problems, go after offenders and do real audits, tie the size of the department to the effort," Heffner says. "We're expecting to see stricter enforcement and more of it – it's self-serving to the agency in charge."

Apgar agrees that tying the auditing and enforcement budget to fines will make for a highly aggressive program. "The number one message coming out of *HITECH* is: Make sure you comply. Compliance is your biggest risk," he says. "HHS was very clear stating that if it provided guidance and you don't follow the rules, then, yes, it'll be out there and it'll be imposing penalties."

But, Melson is quick to point out, *HITECH* isn't just about adding teeth to *HIPAA*. "There are certainly things in it that we as an organization appreciate."

One of those, he says, is the clarification on how business associates fit into the compliance scheme. "*HIPAA* wasn't too clear on that. You could do everything properly, but if your partner made a mistake, it could be interpreted in *HIPAA* that the responsibility lies with the covered entity," Melson says. That never sat too well with Priority Health. "Payers tend to be risk-averse. That's what we do, we manage risk. So knowing that we're not carrying that risk makes us feel better."

Priority Health also welcomes HHS's efforts to standardize encryption processes for protecting PHI, Melson adds.

Working out encryption

In *HITECH*, HHS has determined that PHI will be deemed unusable, unreadable or indecipherable if it has been encrypted – provided, of course, that the encryption key hasn't been broken. It specifies that the encryption must comply with the *HIPAA* Security Rule's provisions regarding EPHI and it recognizes National Institute of Standards and Technology encryption methodologies for data at rest and in motion as the designated means. HHS also instructs on how to destroy media properly in order to render the EPHI incapable of being retrieved. If they follow these guidelines, Healthcare organizations will be provided "safe harbor," meaning they won't be required to provide breach notices to affected individuals, the HHS or the media, the act states.

"This will simplify a number of things for us because it will give us something to validate against and to work with product vendors on," Melson says. "When it comes time to have a discussion about this new product that we're going to use to encrypt transactions between us and a hospital, for instance, everybody can come to the table with the same set of guidelines and if we can all agree that we've met that standard, then we've effectively protected the information."

Of course, many Healthcare organizations already have adapted their security and privacy procedures to meet stringent breach laws enacted in recent years by many state governments – 46 states and one territory have notification rules in place already, according

$19b

of stimulus money pushing forth the EMR agenda in this country

to Apgar. "You could consider *HITECH* a game-changer from a federal oversight and compliance standpoint, but a lot of the things it calls for businesses to do we've already had to address in various state requirements along the way, particularly to meet safe harbor requirements," Melson says.

Priority Health, for example, already uses encryption on thumb drives, hard drives and backup tapes – on anything that, in the event it gets lost or stolen, the stored data is protected, he says. Healthcare organizations that haven't already embraced encryption in such a manner are going to need to do so, and quickly.

But at least in forcing information security officer's hands on encryption, *HITECH* now gives them the budgeting edge, experts say. "Certainly if you tell executive management that what you're facing is notifying individuals, paying fines and ending up in the press, then obviously there's a lot of value to your business to purchase those solutions," says Melson, noting that security vendors are starting to play along nicely, too. "They're making it less expensive and intrusive to add in encryption so it's now a much more palatable option to encrypt computers, especially hard drives and backup tapes, than it was a few years ago."

If anything, *HITECH* has helped information security practitioners, agrees Lou De Frisco, senior technical advisor with New York-based IT consultancy Advantage Technical Advisers. "These types of mandates, while they may be a burden to implement, do help an organization say, 'OK, now we have to follow these certain practices around encryption, privacy and security.' And it helps get buy-in for the proper funding and resources needed to carry the project forward," he says.

At WDH, Heffner is working out how best to embrace safe-harbor encryption methodologies. The facility has some encryption already, but not nearly enough to meet long-term requirements, he says.

"As I talk to vendors, their stance is basically, while you're waiting for the final *HITECH* rules, work at limiting your attack surface. Do a discovery to find out where your PHI and PII [personally identifiable information] lives so you know what you have to protect, and limit the amount of different locations – servers, networks, whatever – you have to defend so that when the rules do come out, you can quickly apply whatever you need to in order to protect it," he says.

Toward that end, for example, WDH is working on knocking down the number of its servers containing patient data from 250 to 100, or even half that, Heffner says. "Any others not hosting or storing PHI or PII, we don't have to hold to the same standard. That's not to say we won't protect them, of course, but we will prioritize the servers that have patient data."

> "Security awareness training...never seems to be completely finished."
>
> *–Mark Olson, IT security manager, Beth Israel Deaconess Medical Center (BIBMC)*

HITECH also could change desktop decision-making, he adds. "We're supposed to encrypt sensitive data on all laptops. Great. One of the best ways to address that is to virtualize them. So do we undertake a virtual desktop/laptop project and get seed capital or do we use some other encryption technology in the short run?," Heffner wonders. "We've got to think about which battles to fight now and which to put off until the final rules come out."

A dose of reality

That speaks to the rocky road Mount Sinai's Contino envisions is ahead for the digitization of health records in a *HITECH* world.

"I don't think the Healthcare or vendor communities at large are ready to act and mobilize as fast as the federal timelines would have them," he says.

362m

mobile devices are projected to be sold in 2010.

– Gartner

Let's face reality, he suggests. "In Healthcare, in terms of technology innovation, we haven't seen a whole lot when it comes to IT for medical records management. While other industries have automated away from paper processes, Healthcare mostly hasn't. So we're not starting with an industry that has a lot of electronic systems in place and is savvy about electronic processes. Instead we're taking a fragmented paper process and moving it forward, and trying to do so at light speed."

Given that reality, slip-ups are all but inevitable, experts agree. "Where we're headed with EMRs makes sense, and I want to see this happen," De Frisco says. "We have major problems in our Healthcare system, mainly from a cost-perspective. If all our processes were electronic and disparate systems were integrated, and if we had a better identity management system for people, and the information was protected and flowed smoothly, we could easily reduce costs and apply those dollars to provide better care to our people. But I'm concerned about what the impact might be of patient information leaking out – and it's a given that it does happen."

That's one of the reasons why under *HITECH*, incident response and investigation becomes hugely important, Melson says. "The biggest change that we've experienced, or at least the way we've refocused as a result of *HITECH,* is how we respond to and investigate issues," he says. "We're definitely running a tighter ship and we're not just looking at 'Did we come to the right conclusion and did we have the right response?' We're focusing on the thoroughness of the investigation and the timeliness of the response."

Those types of details, which Priority Health is able to pull out of its security information and event management tool from ArcSight, are critical when reporting incidents to HHS, he says. "Even if we can demonstrate there's no harm done, it's the ultimate arbitrator of that determination, so we have to provide all those details."

Given the rise of *HITECH*, Melson says he's glad Priority Health had the foresight to begin building an incident response team in 2006. "We saw that was where security was starting to head, and now we have the tools, capabilities and practices in place that let us quickly respond to and learn from incidents as we go." ■

Beth Schultz is a longtime IT writer based in Chicago. You can reach her at bschultz5824@gmail.com.

Beyond *HITECH*

Electronic medical records, access rights and mobility are among the most challenging security issues in health care today, reports Beth Schultz.

Since the federal government's *Health Information Technology for Economic and Clinical Health* Act or *HITECH Act* became law early last year, the Healthcare industry has been in a tizzy about how best to meet stringent new security and privacy guidelines. But keeping protected health information safe is far from the only security challenge whirring around hospital corridors.

In interviews with *SC Magazine,* Healthcare IT security professionals shared other security challenges weighing on their minds. These include concerns over electronic medical records (EMR), security training and access rights management and mobility, for instance. Here's a look inside some of their concerns.

The EMR conundrum

Paul Contino, vice president of IT at Mount Sinai Medical Center and Mount Sinai School of Medicine in New York, says he is particularly worried about the industry's rapid EMR adoption and what that means from a security perspective. The Obama administration wants the majority of Healthcare orga-

$1.5m

annual penalty can be imposed by HITECH Act

nizations – 90 percent of all clinicians and 70 percent of all hospitals – off of paper and using EMR by 2011, and has tied stimulus funding to the effort.

"The problem is, right now when you look at Healthcare, 80 to 90 percent of it, in terms of medical records, is on paper and it's fragmented, sitting in file cabinets in doctors' offices or in hospital basements. Moving to EMR is a positive step forward, but if we're not careful we'll be moving from paper fragmentation to electronic fragmentation," says Contino. And, he adds, such a situation would prove detrimental to the federal government's long-term vision of creating a national Healthcare infrastructure.

"If we're going to spend $19 billion on EMRs, we'll probably have to spend another $19 billion just trying to link all the records together," he says.

> "There are not enough security awareness education programs in Healthcare..."
>
> – Nathan LaFollette, CEO, iNet | Detect

"This process needs to happen," Contino asserts. "We need to move forward with EMR in this country, but we have to be very careful about what we're setting ourselves up for. Just having EMRs without having things like identity management, patient identifiers and practice identifiers – some way of linking the records together – is going to cause a problem and directly links to issues of security and privacy."

While Contino actively espouses the notion of some sort of national, neutral third-party identity management clearinghouse of sorts that would enable the safe, secure linking of EMRs among organizations, he's laying the groundwork for interoperability within his own organization.

In conjunction with working on its EMR implementation, Mount Sinai has developed a smart card program for patients. Program participants will receive photo ID cards containing a microprocessor that, when swiped at registration, would provide access to the patient's insurance information, plus link to medical records throughout the Mount Sinai system. Ultimately, Contino says, patients would be able to use this vetted credential not only with the Mount Sinai system, but, via a trusted authority, across multiple institutions.

"Even if the records aren't electronically linked at this point, a caregiver at another hospital would at least know your EMR number at Mount Sinai as presented on a card that the patient owns," he says, noting that the medical center considers this a proof-of-concept of a federated model for identity-linking that could be taken regionally, statewide and national. "And, since the card is something the patient owns and controls, that's a much more satisfying position for privacy groups."

Mount Sinai has been working on its HealthID smart card concept for years, with the latest iteration, worked on with Fort Wayne, Ind.-based Extension, recently having received endorsement from the American Hospital Association, Contino says. "We're at the point where we'll start implementing cards in mass at Mount Sinai. We've got 100,000 HealthID cards produced here," he says.

With the patient smart cards, Mount Sinai hopes to eliminate the potential of creating duplicate medical records for a patient and the comingling of records of same-named persons. Downstream, the smart cards also will help caregivers deliver better information to billing systems, which in turn means fewer claims declined and shortened revenue cycles.

Educating users on access rights

At Boston's Beth Israel Deaconess Medical Center (BIBMC), a teaching hospital of Harvard Medical School, educating users about security best practices has been an ongoing challenge, says Mark Olson, IT security manager for the institution. "Most of the things that represent a large challenge for us

90%

of all clinicians will be off of paper and using EMR by 2011, if the Obama administration can steer policy

are centered on staffing education and general security awareness training. That's something that never seems to be completely finished or you can never do enough of," he says.

Nathan LaFollette, CEO of iNet|Detect, a security consulting firm in Cleveland, agrees that people processes are a weak link. "Most data compromises occur because an employee who is supposed to be protecting your information has either clicked on an internet link they shouldn't have and has downloaded ransomware, or will fall victim to a social engineering experiment," he says. "There are not enough security awareness education programs in Healthcare in general or with *[HIPAA]* mandates in particular. There are too many policy-compliance mandates and not enough technical control and awareness mandates."

BIDMC is acutely aware of the challenge, Olson says. "It overlays the other problems we're faced with, things like making sure we have adequate access rights management controls in place."

Proper training and good education help mitigate that and other security challenges, he says. For example, administrators, supervisors and department heads should all understand that when physicians move from the cardiac intensive care unit to urology, they need access to new systems and participation on different email lists.

"They need to ensure that the rights of somebody who moves from one role to another at the institution are properly vetted, removed or added," Olson explains.

While user education is one answer, automation is another. The more automated access rights control becomes, the better, Olson says. And, toward that end, BIDMC is working toward automating the auditing of membership by groups.

"We're driving toward a mechanism that says, 'You, as owner of this group, have been educated and trained on who should have access to this group's systems. On a periodic basis, you're going to have to validate that the people on the access list are still appropriate, and if we don't hear from you in a certain amount of time, we'll remove them," he says. "We want to push the management responsibility out to those who should know what the answer is. It's a monumental effort to do that for 14,000 people, but a department head should be able to do that for 300."

Further out, automation could help provide checks and balances. "We can write a back-end auditing script that says, 'If there's been no change to an access list in six quarters, do a manual audit," Olson says. "We're a year or two away, but these are the kinds of programs we want to be able to use."

Mobile patient care

In addition to security training and access rights, mobility also is on BIDMC's laundry list of security projects, Olson says.

"Cleary, mobile devices are part of our culture, and as new residents come into the institution, they're going to have expectations of getting to whatever they want through their iPhones or Droids by browsing," says Olson. He adds that he's concerned that once within the medical center, those devices can then jump on the Wi-Fi network and access internal sites and synch email, for example. "There's not a good strategy to mitigate the risk they represent. Still, banning them from use isn't an effective option. That just can't be done."

And while BIBMC has implemented Research in Motion's BlackBerry Enterprise Server to provide enterprise security controls around use of that smartphone, it hasn't found an adequate solution for devices other than BlackBerrys, Olson says.

"We need to figure out how to integrate them tightly into our infrastructure and make them a useful tool, but provide more support and more risk mitigation as opposed to pushing them away," he says. "We have to find a compelling service or application that is so attractive to them that they'll let me put a VPN client on their device in order to get to it," he adds. "I don't know what that is, but we'll think of something. We're clever."

97%

growth in 2010 in the worldwide market for mobile devices with touchscreens

– Gartner

And in the meantime, he circles back to a reliance on security training and awareness. "We make sure people know what risk their devices present and how to handle and use those properly, including letting us know if they've been lost or stolen," he says.

Kindred Healthcare, a Louisville, Ky.-based company that operates hospitals, nursing centers and a contract rehabilitation service, has taken a different tact to enterprise mobility. By outfitting its therapists with HP iPAQ handheld computers for patient-side data entry, the company has eliminated cumbersome paper processes. It ensures the security of data on those devices using a backend device management and security platform, Sybase's Afaria, says Keith Bickett, project manager for Kindred Healthcare-Peoplefirst, the rehab services business unit.

In this way, Kindred can assure that sensitive data on the device is encrypted and security policies centrally enforced. For example, IT can lock down devices remotely and ensure that only supported applications are installed. Rolling out handhelds to 7,000 therapists would have been impossible without such backend controls in place, Bickett says.

Overall, he adds, enabling point-of-care data entry improves the company's overall security posture.

"All the patient data is contained on this password-protected device and it is encrypted," Bickett says. "That means no more clipboards lying around with patient records on them. There's a lot less likelihood of people seeing information and of patient data getting into insecure hands." ■

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

Masthead

EDITORIAL
EDITOR-IN-CHIEF Illena Armstrong
illena.armstrong@haymarketmedia.com
DEPUTY 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/DIGITAL CONTROLLER
Krassi Varbanov
krassi.varbanov@haymarketmedia.com

U.S. SALES
ASSOCIATE PUBLISHER, VP OF SALES Gill Torren
(646) 638-6008 *gill.torren@haymarketmedia.com*
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*
NATIONAL INSIDE SALES EXECUTIVE Brittany Thompson
(646) 638-6152 *brittany.thompson@haymarketmedia.com*

McAfee SaaS

As part of the world's largest security-dedicated vendor in the world, McAfee SaaS is a leading developer of cloud-based security solutions. McAfee SaaS offers the industry's most comprehensive, cloud-based security portfolio, including email and web protection, message continuity and archiving solutions. McAfee's true multi-tenant, massively scalable SaaS architecture delivers enterprise-grade performance and reliability without enterprise-level complexity and cost.
For more information, visit www.mcafee.com.

Vormetric

Vormetric is the leader in transparent, high-performance encryption for databases, servers and storage. More than 500 of the world's most trusted brands and government agencies have selected Vormetric's application and database transparent solution to simplify and unify encryption, separation of duties and key management across mission-critical heterogeneous systems.
For more information, visit www.vormetric.com.

ArcSight

ArcSight is a leading global provider of security and compliance management solutions that protect businesses and government agencies. ArcSight identifies, assesses and mitigates both internal and external cyberthreats and risks across the organization for activities associated with critical assets and processes. With the market-leading ArcSight SIEM platform, organizations can proactively safeguard their assets, comply with corporate and regulatory policy, and control the risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage.
For more information, visit www.arcsight.com.

CREDANT

CREDANT offers the flexibility to choose the encryption solution that best meets your data protection and compliance needs. Delivering data encryption across any endpoint – desktops, laptops, handheld devices and removable media – including our patented, intelligent data encryption solutions, as well as hardware- and software-based full-disk encryption offerings.
For more information, visit www.credant.com.

Is The Cloud safe for HEALTHCARE?

How Embracing the Internet, Not Avoiding It, May Provide Better, Cheaper Protection

McAfee®

Cloud computing solutions are all the rage. And for good reason.

According to industry analysts and experts, sales of cloud-based computing solutions are expected to far outpace traditional hardware and software solutions. Industry research firm Gartner predicts that applications delivered from the Internet will grow five times faster than traditional software applications through 2013.

Most computing experts agree that these tremendous growth projections are **largely being driven by the economy and the increased pressure on IT organizations to spend less, while doing more**. As a result, more and more organizations of all shapes, sizes and industries, are turning to cloud-based solutions because of their utility-like, pay-as-you-go pricing. When IT needs more computing power, it simply buys more. When it needs less, it spends less. In addition, cloud-computing solutions eliminate the need for huge capital investments in hardware and ongoing maintenance or service fees.

Is The Cloud Safe?

Despite these compelling economic benefits, the question on most people's minds is, **"Is the cloud safe?"** Nowhere is this more true than amongst those in highly regulated industries such as healthcare and financial services, where privacy and security are top concerns.

The simple answer to the question is, "Yes, the cloud is safe." In fact, **the cloud may be even safer than doing it yourself.** Recently published research from Aberdeen reported that users of cloud-based email security solutions experienced 47 percent less cases of malware and 65 percent fewer audit deficiencies than those who used on-premise solutions.

On-premise solutions require adequate resources, expertise, and commitment to manage. So the next logical question most IT managers have to ask is, "Do I have the resources and time to manage the security of my network – or a piece of my network – better than a third-party cloud provider?" In most cases, the honest answer – albeit unpopular – is no. **Few organizations, be it healthcare or otherwise, can match the security expertise, resources, and technology infrastructure of a security technology vendor.**

Take a simple example like email security. Traditionally, organizations would purchase and install hardware or software solutions to filter out spam and email-borne viruses. But spammers are quick to find ways around and through existing filters. Add on top of that all the new technologies, mobile devices and social sites out there, and the list of potential vulnerabilities seem endless. As a result, constant attention and management is required to keep any on-premise solution up-to-date and effective with the latest security patches and downloads.

With cloud-based email security solutions (aka – Software-as-a-Service) like those provided by McAfee and others, the ongoing maintenance and management is handled by the provider. For example, McAfee® SaaS Email Protection service is monitored and managed 24 hours a day, **leveraging threat research collected and correlated in real time by millions of global sensors and more than 350 full-time threat researchers and security analysts around the world.** Few organizations in the world can apply that level of attention and resources just on email security.

Slide Versus Jump Into The Cloud

While many organizations have jumped into cloud-based computing with both feet, the vast majority of organizations do it more gradually. According to Forrester research, 21 percent of enterprises in 2009 were using or piloting cloud-based solutions. That percentage is expected to climb to more than half by the end of 2010.

For many organizations, **email and web security is often a good starting place**, as cloud-based solutions can have an immediate impact on both capital expenditures and ongoing administrative costs. Email and web are also the most common threat vectors used by hackers. They also account for a large percentage of data loss.

Cloud-based email security solutions, like McAfee SaaS Email Protection, work by redirecting an organization's inbound and outbound email traffic through McAfee. Incoming email is first analyzed by McAfee, blocking all spam, viruses and malicious traffic, before being safely and securely delivered to your network. Conversely, McAfee scans all outbound email to enforce policies set by the organization to prevent intentional or unintentional data leaks or privacy breaches. Similarly, McAfee® SaaS Web Protection service protects inbound and outbound Internet traffic by checking for known viruses, malware or malicious IP reputations.

In either case, **the services provide the most up-to-date protection money can buy**, monitored and updated 24x7x365 by a staff of security experts and researchers at McAfee.

Pick the Right Vendor

Whether you're considering one or many cloud-based solutions, the key is picking the right vendor. In many ways, it's no different than choosing a hardware or software vendor. The big difference with picking a cloud-based solution provider, however, is experience and breadth of offerings. There are many one-off vendors who specialize in one cloud-based solution, but not another. And some vendors are relatively new to cloud-based solutions with little or no established track record of reliability and expertise.

McAfee®

More Information:
www.McAfeeSaaS.com
info@McAfeeSaaS.com
877-695-6442

VORMETRIC

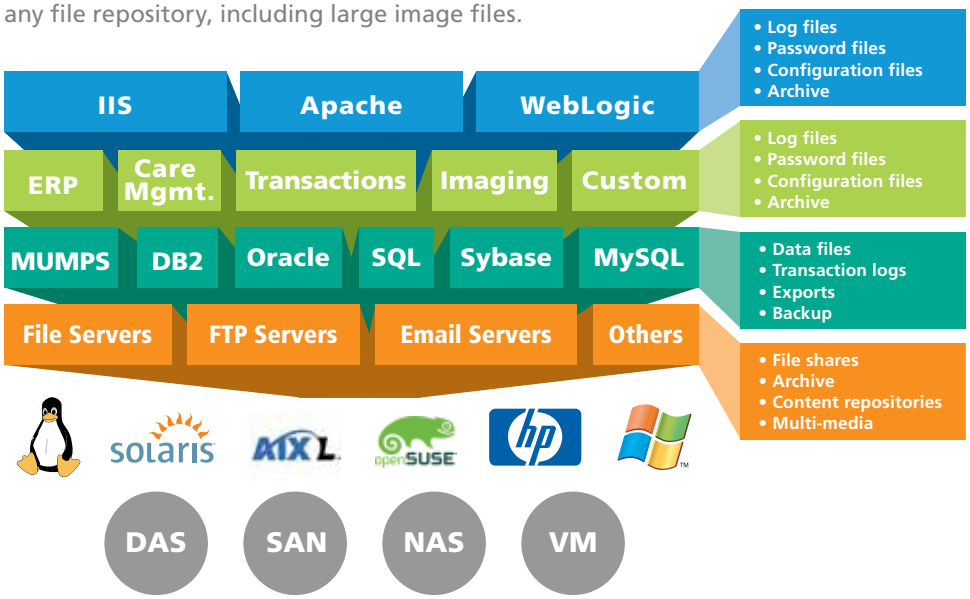
Vormetric Data Security

Simplify Encryption for HITECH Act and HIPAA

The regulatory environment of 2010 creates strong incentives for healthcare organizations to encrypt data. However, when encrypting enterprise systems, performance, integration and key management concerns quickly arise. Exacerbate these issues with Health and Human Services (HHS) requirements–including key security, centralized management, and understanding different encryption approaches for different systems–and encryption across applications, databases, servers and storage can appear impossible.

Vormetric Cures HITECH Encryption Woes

Vormetric Data Security offers a centrally managed, consistent, transparent and high performance approach to encrypting data on any server, database, or storage system without the integration or key management headaches. Vormetric meets all HHS encryption requirements through a policy-based method that provides strong separation of duties for data security and key management. Vormetric encrypts data within clinical systems, for any commercial or proprietary database and for any file repository, including large image files.



Vormetric Data Security benefits for HITECH Act include:

- Strong encryption without the need to alter applications and databases
- Rapid deployment, in most cases installing in less than a week
- Ideal architecture for distributed environments
- Centralized, secure and integrated key management
- Meets HHS encryption requirements for HITECH Act Safe Harbor

Vormetric Meets Healthcare Encryption Needs	
FIPS Certified Encryption	✓
Secure Key Management	✓
HHS and NIST 800-111 Reqs	✓
Proven Performance	✓
Encryption + Access Control	✓
Audit	✓
Separation of Duties	✓
Low TCO	✓
Rapidly Deployable	✓

CLICK TO LEARN MORE

HITECH Act Resource Center

- Register for HITECH Act Webcast, hosted by legal experts
- Download Guide to HITECH Act Encryption

HITECH Act Encryption Case Study

One Fortune 500 healthcare provider with HHS requirements, two month encryption deadline, two-thousand databases.

PROBLEM

A Fortune 500 healthcare provider had two months to deploy encryption for over two-thousand databases, under a custom application in a distributed environment. The encryption system had to meet HHS requirements for HITECH while ensuring minimal impact to database performance, management and application support.

SOLUTION

After understanding management and compliance barriers to native encryption, this company turned to Vormetric Data Security for centralized management, rapid deployment and the ability to meet HHS requirements for separation of duties and key management.

RESULTS

- Met aggressive nationwide compliance timeline without database or application changes
- Consolidated management and audit of massive deployment
- Acquired HHS-compliant enterprise-standard for encryption

Vormetric, Inc. 3131 Jay Street Santa Clara, CA 95054, USA • 888.267.3732 • www.vormetric.com

GET A HIPAA LIFELINE

WITH ARCSIGHT

Your job is to take care of your patients. Our job is to protect your patient's data.

Find out how the ArcSight SIEM Platform for healthcare will protect your organization from privacy violations, and ensure HIPAA audit readiness.

ArcSight SIEM allows you to:

- Safeguard ePHI records and avoid privacy breaches
- Reduce the operational cost of compliance with HIPAA and other regulations
- Decrease healthcare administration costs

Learn why leading healthcare providers and payers, as well as the United States Department of Health and Human Services – who itself mandates HIPAA – rely on ArcSight to protect their organizations. For more information about healthcare security solutions by ArcSight go to **www.arcsight.com/hipaalifeline**

ArcSight

ArcSight Headquarters: 1-888-415-ARST

IS YOUR **DATA PROTECTION** AILING?

SAFEGUARD AGAINST A DAMAGING DATA BREACH.

Ensure HITECH & HIPAA compliance with CREDANT Mobile Guardian.

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® Mobile Guardian® enables you to easily define and enforce security policies from a central console to help you ensure HITECH & HIPAA compliance.

Find out why a growing number of healthcare institutions rely on more intelligent data security. Get valuable information about the new realities facing healthcare organizations, download *The Next Generation of HIPAA and Data Protection in the Healthcare Industry* at **www.credant.com/healthcare**

CREDANT®

We Protect What Matters

www.credant.com

866-CREDANT (273-3268)

DETECT | ENCRYPT | **ENFORCE** | MANAGE | **AUDIT**