



WHITE PAPER:

The Next-Generation of HIPAA and Data Protection

In the Healthcare Industry



Table of Contents

HEALTHCARE INDUSTRY: The Next-Generation of HIPAA and Data Protection



Introduction

The Next-Generation of HIPAA and Data Protection in the Healthcare Industry	3
---	---

Real-World Experiences

Real-World HIPAA Compliance Gaffes	4
--	---

The True Costs

The Costs Associated with Not Protecting Data	5
---	---

Today's Realities

HIPAA Compliance Realities for Today's Healthcare Organizations	6
---	---

The Future of Compliance

Where HIPAA Is Headed	7
The Narrowing Focus on Data Protection	7

Important Considerations

The Role of Security Policies and Enforcement Mechanisms	8
--	---

Responsible Actions

Management Concerns and What Needs to Be Done	9
---	---

Conclusion

Now Is the Time	10
-----------------------	----

Contact Us

.....	11
-------	----



The Next-Generation of HIPAA and Data Protection

With information security and compliance on the minds of many, it seems that the Health Insurance Portability and Accountability Act (HIPAA) has been sort of an afterthought. Until now. As data breaches grow, lawyers are becoming more tech-savvy and politicians are seeing opportunities. The HIPAA Security Rule and Privacy Rule are no longer a set of optional best practices that organizations in the healthcare industry should consider. It's a law once ahead of its time that has now come of age.

Once considered an outdated industry using outdated technologies, healthcare information systems are rapidly maturing. Add to that the complexities of the networked systems we use today along with all the sensitive healthcare data being shuffled around, and it becomes clear that businesses in this industry have their hands full.

Healthcare professionals access electronic Protected Health Information (ePHI) in so many places. In fact, legislation was recently passed in the US pushing for all patient information to be electronic; thus, its presence and use is only going to increase. To ensure reasonable services are provided, ePHI needs to be readily available. But therein lies the problem. There are not only multiple access points but also multiple individuals involved. Having healthcare data anywhere and everywhere broadens the areas of exposure, ultimately creating compliance gaps and introducing business risks.



It's been proven time and again that standalone and siloed controls or leaving it to the end-user to police themselves are not the answer to compliance and security. Data protection in today's healthcare environments requires comprehensive controls that are proactive, well thought-out and managed with care and common sense. This paper contains some practical advice on processes and controls you can use to gain the visibility and control needed for not only HIPAA compliance but also an effective information security program overall.

Real-World HIPAA Compliance Gaffes

While consulting in the healthcare industry, I've heard alarming statements regarding HIPAA compliance and data protection that can get—and have gotten—healthcare organizations in a real bind. I've heard the following from healthcare administrators, compliance officers, and even network administrators:

- › “HIPAA doesn't apply to us”
- › “Our compliance manager handles all of that”
- › “Our IT folks handle all of that”
- › “We did a checklist audit and didn't find anything of concern”
- › “We have a security policy”
- › “We trust our employees to do the right thing”
- › “Our security assessment from 2 years ago revealed that everything's in check”
- › “We're pretty much compliant with HIPAA, therefore everything's safe and secure”
- › “We have a firewall and use antivirus software”
- › “The HIPAA police aren't going to come after us”

Assumptions such as these tend to reflect the overall culture of security and compliance throughout the organization. They also tend to correlate with the number of business risks uncovered that are related to computers, IT, and sensitive data.

Caution

Contrary to popular assumption, mobile devices (laptops, USB drives, smartphones, iPods, etc.) are by and large not secure. In fact, for many organizations—especially those in healthcare—mobile devices present one of the greatest data security and compliance risks to the business. Unfortunately, most managers have yet to realize this.

According to the Privacy Rights Clearinghouse A Chronology of Data Breaches (<http://www.privacyrights.org/ar/ChronDataBreaches.htm>), eight healthcare-related data breaches have occurred thus far in the first 2 months of 2009, exposing tens of thousands of records. (A perusal of this chronology—which dates back to 2005—along with other breach-tracking databases such as the Open Security Foundation's DataLossDB at <http://datalossdb.org> shows a clear trend that organizations in the healthcare industry are a big contributor to the problem.) And it's only getting worse.

The good news is that organizations tend to learn from their data breach mistakes; however, this is not the most cost-effective way to protect data. Research studies and my own experience have both shown that organizations tend to spend less money in subsequent data breaches (that is, healthcare organizations that have been attacked multiple times). This can be attributed to the implementation of data protection solutions and simply general experience gained. Organizations often come out on the other side of a breach with a stronger culture of security, greater resiliency, and an overall wiser approach to how they address compliance and data protection.



The Costs Associated with Not Protecting Data

Numerous studies on the cost of data breaches have been undertaken over the years. Although there is no way to definitively quantify how much data breaches really cost, ballpark estimates are still beneficial. You can use them not only to estimate what you're up against if a breach does occur but also to educate management about why compliance and data protection need to be on their radar. The exposure of just a few thousand healthcare records can cost \$1 million or more when you factor in incident response costs, consulting and attorney's fees, credit monitoring services, regulatory fines, the short-term lost revenue, and the longer-term lost revenue as trust and confidence in your brand is diminished in your customers' eyes.

Note

For interesting insight into just how quickly data breach costs can add up, check out Rebecca Herold's Privacy Breach Impact Calculator at <http://www.informationshield.com/privacybreachcalc.html> and Darwin's Tech//404 Data Loss Cost Calculator at <http://www.tech-404.com/calculator.html>.

General statistics can be beneficial as well. For example, the Ponemon Institute claims the average cost of a data breach in 2008 grew 11% from 2006 to the current \$202 and up per record compromised. Gartner claims the cost of data breaches will continue to increase through 2009.

Furthermore, the CREDANT Technologies 2008 Healthcare Security Survey (www.credant.com/mailedRegistration/Survey_em.php) of healthcare practitioners in the U.S. found:

- › 49% of those with mobile devices download patient data
- › 71.7% of them depend only on passwords to protect data
- › 21% of them have no confidence in the security of their mobile devices

These numbers are telling from two perspectives. First, it confirms that ePHI is scattered. Second, many organizations are still using security controls that are known to be weak and often easily bypassed. Finally, as I've seen in my work, the majority of people assume that their mobile devices are secure, especially if they're protected only by a password. Again, this is completely untrue.

Caution

Whether specific dollar losses can be calculated and whether management agrees with security surveys, the fact is that compliance and data protection cannot be ignored. Mindsets such as "I just need to run into the store real quick, my laptop will be fine in the car" and "We don't have anything a hacker would want anyway" are not only short-sighted but they're also dangerous assumptions that have put many healthcare providers in the hot seat in recent years. A spotlight you likely don't want to be in.



HIPAA Compliance Realities for Today's Healthcare Organizations

Healthcare providers often gather, process, and store more sensitive information than any other type of business. Hardly any other industry readily collects so much personal information such as:

- › Social Security numbers
- › Addresses and phone numbers
- › Financial details for bank accounts and credit cards
- › Personal and family health history

There has been a general lack of ownership in the healthcare industry when it comes to protecting these sensitive records. Even with the HIPAA regulation mandating protective measures there are still a lot of gaps. Furthermore, with the expansion of IT in healthcare in the new government expansion bill entitled American Recovery and Reinvestment Act of 2009, there is a lot for IT and security managers to think about from this point forward. Furthermore, with the Health Information Technology for Economic and Clinical Health Act (HITECH) – a key provision of the American Recovery and Reinvestment Act of 2009 (ARRA), signed in to law on Tuesday, February 17, 2009, – important changes in privacy and security regulations will become effective one year after enactment of ARRA on February 17, 2010. IT and Security Managers have a lot to think about, and get right, in a very short timeframe.

Caution

There has been a lot of talk about whether healthcare providers even need most of the information they collect from patients. The truth is that in many cases they don't, yet most patients willingly provide it without question. And once this information gets out into the "wild," electronically it spreads with no way to know whether it's protected.

As with any business, unintentional disclosures through careless use and general ignorance are occurring. Malicious attacks from outside sources such as hackers and malware are threats as well. Regardless of the threat source, the reality is that most security vulnerabilities and HIPAA breaches involve not knowing what's where, not knowing if/how it's vulnerable, and not putting even the most basic controls in place. My own experience has shown that most vulnerabilities uncovered are pretty basic yet very detrimental. In fact, most security breaches occur when attackers exploit weaknesses that have a known fix, such as a patch or configuration tweak. Contrary to popular belief, the big security gotchas are rarely advanced hack attacks that only a handful of people are capable of exploiting. Thinking back to the "high-priority" findings in my security assessment reports, they're almost always oversights of very basic vulnerabilities that should've been on the radar of those responsible.

Another area of concern for healthcare organizations is the business associates they work with on a day-to-day basis. There are easily as many business associates along the data path as there are individuals handling ePHI inside the organization.

Note

HIPAA business associates are defined as people who are not members of a covered entity's workforce but provide activities or functions related to the use or disclosure of ePHI.

These business associates have as much responsibility in the HIPAA compliance chain as any of the covered entities do. Yet the only true check-and-balance component is legal verbiage buried deep in a business contract. This leads to the people who are responsible for data protection being out of the loop, and thus the cycle of non-compliance and security risks continues.

The Future of Compliance

HEALTHCARE INDUSTRY: The Next-Generation of HIPAA and Data Protection



Caution

HIPAA compliance and data protection are just as important as any other business function. In fact, they touch virtually every part of the business, so it is important that the right people are involved. Compliance isn't a one-time deal. Compliance and data protection require ongoing TLC on the part of IT, management, and every single user along the way.

Where HIPAA is Headed

Generally speaking, there has been a lack of HIPAA enforcement on the part of the Department of Health and Human Services (HHS) since the Security Rule was enacted in 2003. Even after the Centers for Medicare & Medicaid Services (CMS) was put in charge of HIPAA Security Rule enforcement in 2006, there haven't been many strict actions taken. But that's starting to change.

Not long after a report was released from the US Office of the Inspector General about lax HIPAA enforcement on the part of HHS, CVS Caremark Corporation was fined \$2.25 million for a HIPAA privacy-related violation. A sizable sum to pay for careless information disposal practices. Underscoring the need for healthcare organizations to evolve their operations, the recent American Recovery and Reinvestment Act of 2009 also includes several additions to HIPAA regarding breach notification, additional enforcement penalties for HIPAA business associates, and more. Thus, unlike other government and industry regulations—such as the Sarbanes-Oxley Act (SOX) and Payment Card Industry (PCI) Data Security Standard (DSS)—that have gotten the attention of business managers, HIPAA has taken quite a while to gain traction in the healthcare industry. Based on recent events, such as Providence Health & Services being fined \$100,000 by HHS, it appears that HIPAA is growing teeth, so the days of many healthcare organizations not taking it seriously may soon be over.

As consumers become more aware of what is at stake (what they have to lose and what they have to go through to fix the resulting issues), we'll start seeing a culture that demands information privacy and security. This will likely be in the form of increased demands on politicians to grow compliance requirements—way more than what we have today.

Even with increased enforcement, data breaches will continue. When a breach does occur, being able to prove that reasonable controls were in place will become paramount. Savvy business managers will focus on not only on the 18 HIPAA Security Rule standards but also information security as a whole. Once a solid information security program is put into place, businesses can fall into compliance with practically every data protection law or regulation that comes their way.

The Narrowing Focus on Data Protection

There has been a recent shift towards protecting data especially when it's stored on so many different systems. Traditionally, we've thought of data protection as a big database protected by a fancy firewall. It's not that simplistic any more. ePHI is literally scattered across multiple systems—all across the enterprise. From desktop computers to laptops to smartphones, USB memory sticks, iPods and PDAs, there can be thousands of islands of data within any given organization containing thousands of records. Furthermore, ePHI is at rest most of the time. This situation provides ample opportunity for both curious and malicious insiders and outsiders alike to gain access.

Sensitive healthcare data is not only scattered about multiple computer systems, it can be accessed and stored in many different ways:

- › Remote storage devices connect through USB and FireWire ports
- › Wireless protocols such as Wi-Fi and Bluetooth

Important Considerations

HEALTHCARE INDUSTRY: The Next-Generation of HIPAA and Data Protection



- › Hardwired connections such as Ethernet ports, PC card slots, and parallel ports

Gaining control of this sensitive data is one of the greatest IT problems healthcare organizations face. Everyone from network administrators to security managers to compliance officers seems to be struggling with just what to do to keep everything under wraps. Many of our past protective measures for keeping data locked down and secured such as basic passwords, access rights, and encrypting entire drives aren't working. In reality, in order to get your arms around security in the context of HIPAA compliance, a new mindset is required. Looking at HIPAA compliance from the perspective of data protection allows you to focus on what matters most.

Caution

Pay special attention to shared computers. They're often a necessity in healthcare environments but such utility and convenience also leads to compliance and data protection gaps. Information stored on a shared computer may not be appropriate for all users on the computer to access. And these systems tend to get less preventative maintenance. Always remember that with shared computing comes decreased accountability because personnel often use their co-workers' already logged-in sessions, thus the compliance and security gaps will widen over time if the issues are not addressed and bad habits are allowed to continue.

The biggest hurdle many people have to overcome is the fact that encryption as we've known it (sector-based full disk encryption) is not enough. In order to achieve HIPAA compliance and maintain realistic security, you have to go several steps beyond basic controls and actually monitor your systems centrally in real time, continually check for policy compliance, and so on. These actions have to be taken not only on your systems while they're in your control but also while they're at coffee shops, hotels, airports,

homes, and practically everywhere in between.

The Role of Security Policies and Enforcement Mechanisms

Nearly half the 42 implementation specifications that make up the 18 standards of the HIPAA Security Rule are "required" and the other half are "addressable" based upon the outcome of a risk assessment. Thus, good documentation and effective technical controls are needed to achieve and maintain compliance and ultimately provide adequate data protection.

The most effective security policies are managed centrally and enforced locally. Centrally managed controls simplify the day-to-day administration. They also tend to snap-in and work well with other network technologies you likely already have, such as Windows Active Directory (AD). Local enforcement mechanisms residing on the actual device ensure that policies are enforced at all times regardless of where the system is located and how it's connected.

There is no one best solution for HIPAA Security Rule compliance or overall information security. That said, if you take your time and ask the right questions, you can find good solutions that take the pain out of the process. Such solutions not only help protect sensitive healthcare data but also help you prove that reasonable controls were in place if there is ever any question. An ideal solution will allow you to correlate events and will not impact your software patching, change management, and overall IT processes. Tools need to be selected that have little to no impact on operations and are effectively transparent to your users.

The key consideration to remember is that most policies can't be enforced without using good technologies, and many technologies are worthless if you don't have reasonable policies documented to back them up.



Management Concerns and What Needs to Be Done

You can't fix—nor protect—what you don't acknowledge. The first step down the path to reasonable and effective HIPAA Security Rule compliance is to understand what is really required of your organization. After you work out the applicable details of the HIPAA Security Rule, you've got to follow the widely accepted security methodology that has been proven to work:

- › Find out where you're weak and estimate the risk
- › Put reasonable and appropriate policies and controls in place to minimize the risks
- › Log, monitor, and alert on suspect conditions
- › Report your ongoing findings
- › Adjust your policies and controls as needed
- › Repeat

Note

Start small but ultimately focus your efforts in these areas for all ePHI located on all end points at all your locations.

Time isn't going to stop ticking. As we progress, our information systems will become more complex and, as a result, more security issues will arise. The increasing regulations we're seeing will lead to greater consequences and new technologies introduced in the future will only exacerbate the problem and create new problems of their own.

Note

Compliance and data protection should not get in the way of doing business. Doctors, nurses, and other healthcare professionals want to get the most out of their technology rather than be hindered by poorly implemented controls. Focus on minimizing risks while at the same time enabling productivity. This means staying out of the way of users wherever you can. Transparent technologies and reasonable policies are essential elements of this strategy.

Conclusion

HEALTHCARE INDUSTRY: The Next-Generation of HIPAA and Data Protection



Now Is the Time

There has never been a better time to put solid security processes and controls into place. If there is one critical factor for success with HIPAA and compliance in general, it's to focus on data protection at the highest levels possible across the board. Using centrally managed tools that not only have a minimal impact on IT operations but also are transparent to users and provide solid compliance reporting is essential. So, find out where you're vulnerable, implement the right policies and technical controls, and continually assess and optimize. Doing so will not only help you bring your organization in line with HIPAA but also with all the additional regulations you're up against.

– **Kevin Beaver**, is an independent information security consultant, author, keynote speaker, and expert witness with Atlanta-based Principle Logic, LLC.

Contact Us

HEALTHCARE INDUSTRY: The Next-Generation of HIPAA and Data Protection



More information, including data sheets, case studies, analyst reports and additional business and technical white papers are available in the CREDANT Technologies Resource Center. Please let us know how we can help meet your data protection needs:

CREDANT Technologies

15303 Dallas Parkway

Suite 1420

Addison, Texas 75001

1-866-CREDANT (273-3268) or 972-458-5400

www.CREDANT.com

info@CREDANT.com

© 2009 CREDANT Technologies, Inc. All rights reserved. CREDANT Technologies, CREDANT, the We Protect What Matters tagline, the CREDANT logo are, or will be, registered trademarks of CREDANT Technologies, Inc. All other trademarks, service marks, and/or product names are the property of their respective owners. Product information is subject to change without notice.