Improving PHI Security Through Better HIPAA Compliance
Designing a Continuous Response Architecture
Table of Contents

Introduction ...............................................................3
Kevin Beaver .........................................................4
Whats New With HIPAA? .........................................5
How HIPAA Applies to your Business .........................6
Understanding your Level of HIPAA Risk, the right way ....7
Common Sense Incident Response for HIPAA ...............8
Introduction

From the very beginning, the Health Insurance Portability and Accountability Act (HIPAA) has had a far-reaching impact on IT and information security. With the creation of the HITECH Act in 2009 and the Omnibus Rule in 2013, the HIPAA Security Rule requirements are front and center for all organizations – both large and small – that do business in the healthcare industry.

In this four-part e-book, Kevin Beaver, an Atlanta-based information security consultant and co-author of the newly-updated book The Practical Guide to HIPAA Privacy and Security Compliance, 2nd edition will bring you up to speed on the latest HIPAA changes impacting information security and outline some practical steps you can take, starting today, to not only meet HIPAA’s compliance requirements but to also make tangible improvements to your information security program as a whole.

Kevin Beaver

Kevin Beaver, CISSP is an information security consultant, writer, professional speaker, and expert witness with Atlanta-based Principle Logic, LLC. With over 25 years of experience in the industry, Kevin specializes in performing independent security assessments to help businesses minimize their IT risks and take the pain out of compliance. He has authored/co-authored 11 books on information security including the best-selling Hacking For Dummies and The Practical Guide to HIPAA Privacy and Security Compliance. In addition, he’s the creator of the SecurityOn Wheels information security audio books and blog providing securitlearning for IT professionals on the go. Kevin can be reached at www.principlelogic.com and you can connect with him on Twitter and on LinkedIn.
Improving PHI Security Through Better HIPAA Compliance

What’s New With HIPAA?

If you do business in or around the healthcare industry in the U.S., you’re no doubt familiar with HIPAA – the Health Insurance Portability and Accountability Act of 1996. This federal government regulation applies to organizations in the healthcare industry that process or store protected health information (PHI) such as healthcare providers, insurance companies, and even private businesses who manage their own health plans – all of which are referred to as covered entities (CEs). HIPAA has a far-reaching impact on healthcare through its various rules. In the context of IT and information risk, the original HIPAA Security Rule, which amazingly has been in place for a decade, required CEs to take the proper steps to ensure the security of their electronic PHI. But that was just the beginning.

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act tightened down on some of the original HIPAA requirements to ensure that controls and enforcement were properly implemented, including encryption controls, breach notification, and a database that publicly outlines the details of breaches affecting 500 or more individuals. Even with the tighter requirements of the HITECH Act, HIPAA-related security breaches were still occurring. In fact, thus far in 2014, over 100 PHI-related breaches have been publicized in HHS’s database. And those are the known breaches. What else is happening that hasn’t yet been discovered? Needless to say, certain CEs are finding out the hard way that mere policies weren’t enough to protect sensitive information. In my work performing security assessments, I’ve seen the good, the bad, and the ugly in terms of HIPAA compliance or, more appropriately, lack of compliance.

The U.S. Department of Health and Human Services (a.k.a. HHS), the federal agency responsible for HIPAA, saw an opportunity to further tighten down on the HIPAA rules and, in 2013, the Omnibus Rule was born. So, what’s the big deal with the Omnibus Rule? First and foremost, HHS became very prescriptive with whom the HIPAA Security Rule applied to. Early on, a business associate agreement between CEs and those organizations with whom they did business was enough to satisfy the HIPAA requirements.

We’ve all witnessed how contracts mean very little in terms of security breach prevention! Now, it’s been made clear that the specific Security Rule requirements and the HITECH Act apply to all business associates and their subcontractors. Suddenly HIPAA compliance has a much greater reach.

The Omnibus Rule also introduced a few other notable requirements to further enhance security and minimize the impact of breaches as follows:

• Clarification on the definition of “breach” which is the acquisition, access, use, or disclosure of protected health information in a manner not permitted which compromises the security or privacy of the protected health information.
• Post-breach risk analysis requirements where three of the following four items must be met:
  • The nature and extent of the PHI presumed to be breached
  • The unauthorized party who gained access
  • Whether the PHI was actually viewed or acquired
  • The extent to which the risk has been mitigated
• Safe Harbor protection (i.e. no post-breach risk analysis or breach notification requirements) for PHI that can be shown to have been encrypted at the time of breach.

All in all, the HIPAA Security Rule, HITECH Act, and the latest Omnibus Rule requirements are nothing magical or mysterious or even that difficult to implement. They’re common sense, decades-old information security principles that every business should already have in place. The level of scrutiny by HHS’s Office of Civil Rights (the enforcement arm for HIPAA) is likely to grow. I know it can be painful but it’s time to get on board.

Medical data is becoming the next revenue stream for hackers

The personal information found in health care records fetches hefty sums on underground markets, making any company that stores such data a very attractive target for attackers.

- Computerworld, March 20, 2015
A decade or so ago, before IT compliance was mainstream, it wasn’t uncommon to hear business executives proclaim that security didn’t “apply” to their businesses. Well after HIPAA Security Rule enforcement began in 2005, many HIPAA covered entities (CEs) as well as their business associates (BAs) still thought that HIPAA was a mere set of suggestions that only affected others. Only the largest of healthcare providers and insurance companies were making efforts, albeit half-hearted in many cases, to comply with the HIPAA Security Rule’s requirements. It wasn’t until the HITECH Act, and more recently, the Omnibus Rule updates that many CEs and BAs have seen the writing on the wall and have gotten on board with HIPAA compliance.

At this point, covered entities know who they are. I’m still not convinced that BAs are fully aware of what’s required, what’s at stake, or that they even need to comply at all. Many BAs are in the business of making widgets, analyzing data, and processing claims and security is not really their strong point. Whether or not that’s the case, HIPAA’s security requirements apply to their environments just as much as it does to the environments of CEs.

Technically speaking, the original Security Rule required that BAs comply with the HIPAA requirements. However, the way the regulation was written, it ended up being more bark than bite and no one took it seriously. The HITECH Act, and especially the Omnibus Rule have clarified what’s expected of BAs and their subcontractors that process, store, or otherwise have their hands in protected health information (PHI).

Even with the new requirements, I still see many people taking the approach of relying on the traditional business associate agreement to solve security problems. It’s time to go beyond the contract and ensure that all parties in the HIPAA equation are doing what needs to be done to truly secure PHI – from network endpoints to the cloud and everything in between. Business associate agreements are a good fail back plan when something goes awry and accountability (blame) needs to be assigned. Still, there’s no contract in the world that’s going to protect your business from the time, money, and effort required of your executives, PR, IT, legal and related staff – not to mention the hit to your bottom line – when a security breach occurs.

Something that still blows my mind is the fact that certain CEs who have been required to be in compliance with the HIPAA Security Rule for a decade have yet to do anything to truly address the spirit of the requirements. Sure, most organizations have policies but those are usually worth less than the notebook that they’re stuffed inside. Many organizations have core technical controls in place but they’re often not well implemented or managed. It’s more like they’re there for show to appease any auditors who might ask for a report. Surprisingly, some organizations don’t even have the basic security controls in place that we’ve know about for years. I recently met someone who works for a large and well-respected healthcare organization who said they’re just now rolling out anti-virus software!

If your business is considered a HIPAA CE, a BA, or a subcontractor of a BA and you’ve yet to get rolling with HIPAA security compliance, you have to get started today. The good news is that it doesn’t have to be that difficult. Ensuring the security of your PHI as well as ongoing HIPAA compliance can be boiled down to three functions:

- Knowing what you’ve got
- Understanding how it’s at risk
- Doing something about it

You can start now by getting to know your network better, especially where PHI is stored and flows throughout the environment. Interestingly, most IT pros have no clue where their structured and unstructured information resides. I first wrote about this problem over eight years ago and apparently it’s worse than ever. That’s bad for compliance but, more so, it’s bad for business. You cannot secure what you don’t acknowledge. Acknowledging that HIPAA applies to your business is the first step.

HIPAA Violation Costs Facilities $4.8 Million

This May, the Department of Health and Human Services set a record...

- MD News, August 27, 2014
Improving PHI Security Through Better HIPAA Compliance

Understanding Your Level of HIPAA Risk, The Right Way

When it comes to information security and HIPAA compliance, if you choose to ignore the risks your organization faces, you’re going to have to live with the consequences. Interestingly, I’ve found a common theme across HIPAA covered entities (CEs) and their business associates (BAs), regardless of their size and security budget: they already have much of what’s needed in place to meet the HIPAA Security Rule and subsequently, the HITECH Act and Omnibus Rule requirements including:

- Compliance managers
- Business associate agreements
- Documented security policies
- Disaster recovery and business continuity plans
- Certain efforts around security awareness
- Core security processes that integrate with IT and business functions

The people, documentation, and processes are in place, but oddly enough, many of these organizations have yet to perform a formal information risk assessment – or, as HIPAA refers to it, a risk analysis. These things often exist in a vacuum but there’s no real substance. It satisfies a checkbox but it’s mostly just for show. Therein lies the problem with much of what we know as HIPAA compliance: it’s people going through the motions to comply with a regulation and appease auditors rather than taking a risk-based approach to information security and letting compliance evolve as a result.

Similar to how you can’t build a house without a set of plans or design an automobile without a set of blueprints, there’s no reasonable way the HIPAA security requirements can be put into place – and function properly – without fully understanding what the risks are that they’re trying to address in the first place.

Even more interesting – and dangerous – is the fact that many CEs and BAs have yet to do anything in terms of penetration testing, vulnerability assessments, or technical IT audits. Their PHI is hanging in the balance because Web applications, mobile apps, workstations, servers, wireless networks, and numerous other network systems haven’t gotten the attention they need in terms of in-depth security reviews. Simple vulnerability scans won’t cut it. Neither will assuming that IT support, EMR software, and cloud vendor are doing what’s necessary to ensure everything is kept in check on their end. This is a large reason why the Omnibus Rule’s requirement that all BAs and their subcontractors have to comply with HIPAA came about. There are a lot of information risks that have yet to be acknowledged on their side of the table.

I think many people are so caught up in the compliance madness that they fail to truly understand what information risk is about. It can be defined as the likelihood of disruption, damage, or loss occurring when a threat exploits a vulnerability. Taking that into consideration, you can use it not only in your security assessments but also every decision that’s made around healthcare IT and PHI. You must determine which PHI and related systems are vulnerable, how threats can exploit them, and then implement reasonable security controls to eliminate or minimize the risks. Most importantly, effective information risk management involves common sense and perspective. Not everything that’s uncovered is a risk. However, many things that aren’t uncovered due to improper testing and network visibility truly are.

It’s not all about you – you have to learn from others. Don’t fall into the security theater trap assuming all is well just because you’ve gone through the motions on the operational/administrative side of security. That’s only half the story, assuming it was done properly in the first place. Chinese military general, Sun Tzu, once said “Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.” You can’t afford to approach HIPAA in this way.

Even if you believe your security program is solid, there’s always room for improvement. There’s a 100 percent chance that something, somewhere on your network needs attention. It may be people-related, something with a business process, or something technical lurking in your environment. Only you will know. Looking at the positive, you’re likely already doing many things well in terms of information security. The risks that do surface can be easy to resolve if all the right people are on board and politics doesn’t get in the way. Perhaps the best side-effect of all is that if you take a risk-based approach to information security, you’ll have a much more secure environment and, out of nowhere, “compliance” will emerge as a result.

A 2014 audit by the OCR HHS found “no complete and accurate risk assessment in two-thirds of healthcare entities:”

- 47 of 59 providers;
- 20 out of 35 health plans;
- 2 out of 7 clearinghouses

**Key Takeaway:**

Most covered entities have not identified the risks and vulnerabilities of their environment, and therefore are failing to adequately safeguard PHI.
Improving PHI Security Through Better HIPAA Compliance

Common Sense Incident Response For HIPAA

At a minimum, your incident response plan should cover the following:

- Overview
- Roles and Responsibilities
- Incidents Requiring Action
- Detection, Investigation, and Containment
- Eradication
- Recovery
- Call List
- Testing and Revisions

You want to be able to rely on your plan to help you respond (not react) in a mature and professional way to answer the important questions:

What has happened?
How did it happen?
What was impacted?
Who was involved?
What are the next steps?

With all the time, effort, and money you put into HIPAA compliance, the last thing you want is to get caught off guard with a breach, malware infection, or similar incident you’re not prepared to handle. Reality is teaching us that no matter how much is invested in security, negative events are going to occur. That’s okay, as long as you’re prepared to respond in reasonable ways. Compliance and information security are not about eliminating all threats and vulnerabilities but rather what you do to minimize the impact of the risks when the going gets rough.

Greek philosopher Epictetus once said “Circumstances don’t make the man, they only reveal him to himself.” As soon as a security incident occurs, your testing time begins. During and after an incident, your peers and many others around you will be watching you to see how you respond.

Every choice regarding security and compliance you’ve made up to that point will either pay off in positive ways or work against you.

First things first, if you’re going to effectively respond to incidents you’re going to have to know your environment. There’s more to what you’re hearing and seeing. Given the complexity of the average network, it can be impossible to keep up with the deluge of system events being thrown your way, all the sensitive information scattered about on your endpoints, and all the network connections entering and leaving your environment that may or may not be legitimate. The question becomes: do you really have control over the important things? This starts with knowing your information systems environment and how it’s currently at risk.

Another critical aspect to incident response is to have a well-documented plan. Interestingly, many organizations I see (especially in healthcare) don’t have one. Most have a disaster recovery or business continuity plan but not one that deals with security incidents involving things that can get your business into a crunch such as malware outbreaks, external hacking, insider abuse, and lost/stolen laptops.

Perhaps the wisest approach to incident response is to step back and ask yourself what the worst is that can happen and then do whatever it takes to ensure it doesn’t happen. Business schools teach this concept – it’s called mini-max regret analysis. You want to minimize your maximum regret. Finding and eliminating the low-hanging fruit on your network and utilizing the proper security technologies are key to doing so.

Don’t try to address everything at once. Focus your incident response plan on your most critical systems and information (PHI in the case of HIPAA compliance) and then build it out from there. The important thing is to get started. Winston Churchill said “Want of foresight, unwillingness to act when action would be simple and effective, lack of clear thinking, confusion of counsel until the emergency comes...these are the features which constitute the endless repetition of history.” You can’t afford the journey down that path – not only for the sake of compliance but, just as importantly, for the sake of your business and your career.

Healthcare Data Breaches Can Push Patients Away, Says Survey

Healthcare data breaches can be devastating for patients and the healthcare facility that was attacked. The organization could face severe penalties from the Department of Health & Human Services (HHS) if it is deemed that it violated HIPAA, while patients could spend years working to recover from having their personal information accessed.

About Carbon Black

Carbon Black is the leading provider of a next-generation endpoint-security platform designed to enable organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 650 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute’s Best of 2015 Awards.

2017 © Carbon Black is a registered trademark of Carbon Black, Inc. All other company or product names may be the trademarks of their respective owners.