WHITE PAPER

HIPAA: Beyond Compliance

Why Compliance Alone Won't Protect You From a Security Breach

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction 2

Why HIPAA-Compliant Organizations Remain At Risk 3

One Size Does Not Fit All When It Comes To Security 3

You Lack Sufficient Resources to Properly Scale the Security Program 3

Competing Priorities Get In the Way of Adequate Workforce Training 4

“We’re a Small Fish - Who Would Target Us Anyway?” 5

How to Go Beyond HIPPA and Protect Your Organization 6

Invest in a Security Program - Not Just a Compliance Checklist 6

Keep Workforce Training at the Top of Your Priority List 7

Ensure that Security Processes and Procedures Take Into Account Real User Behavior 8

Implement the Right Technology to Augment Limited Resources 8

Back Up Early and Often 10

Find Out How One Company Used These Tips to Mature Their Security Program 11

Introduction

If you're an information security (IS) professional working in the healthcare space, HIPAA (the Health Insurance Portability and Accountability Act) is at the forefront of your mind with everything you do. But if your organization cares about preventing security breaches, staying in operation, and maintaining patient trust, HIPAA compliance is not enough. For years, we have seen organizations say that they are compliant with IS regulations, and then we have seen the same organizations suffer a major security breach. Why is this the case?

In this white paper, we explain the shortcomings of HIPAA pertaining to cyber security; how compliance with HIPAA regulations is not enough to secure information; and what healthcare organizations can do to go beyond HIPAA and keep their enterprises protected.

Why HIPAA-Compliant Organizations Remain At Risk

Maybe you've been through an audit already. Or, you feel confident that you would do well if you were selected for one. Ideally, that means that your organization's risk of a data breach or malware attack is minimized, but that's often not the case. Here are the top reasons that HIPAA-compliant organizations remain at risk.

One Size Does Not Fit All When It Comes To Security

Compliance frameworks like HIPAA are designed to be one-size-fits-all when it comes to defining necessary controls for organizations. This might not be a problem for enterprises that have the appropriate funding, experience, and resources to customize the framework to their specific needs. But when organizations that don't have these luxuries try to implement the frameworks, they often struggle to do much more than meet the basic requirements laid out for them. They may be able to achieve enough to pass an audit, but regulatory fines are only one threat of many. Even when the auditors are satisfied, a compliant organization can remain at risk for a major security breach.

You Lack Sufficient Resources to Properly Scale the Security Program

Developing an IS program takes time, resources, and support from the entire organization – especially senior leadership. Often, an IS program has to be built incrementally over time. Although not everyone needs to achieve the most advanced capabilities in all areas of information security, time is required to develop each aspect of the program to a level appropriate for the organization. This could mean multiple quarters or even years to properly implement every aspect. Regulatory compliance programs, on the other hand, are intended to cover all aspects of information security from day one. This creates a conflict, as it incentivizes decision makers to get the compliance “check mark” by minimally implementing all of the controls required to get a clean audit, without ensuring that they are fully effective or the right thing for the company. Leaders are often measured by how well they do in an audit, not how well they are protecting the business.

In addition, most organizations face another hurdle outside of their control: competition for skilled talent. IT talent shortages are a common complaint across industries, and experts don’t see this problem going away any time soon. Good IS staff are expensive, hard to find, and constantly moving around between companies. This makes it difficult for small IT teams to hire and retain staff capable of properly interpreting and implementing a right-sized information security program.

Competing Priorities Get In the Way of Adequate Workforce Training

The biggest risk for data breaches remains the people within the organization. That means everyone, from management on down through the workforce. This includes those whose official duties do not appear to have a direct security component, but whose day-to-day responsibilities have them accessing systems that are vulnerable to attack without the appropriate level of awareness and safeguards. It takes just one employee's slip-up to compromise an entire system.

Spear phishing and other similar techniques are still the most common points of entry into organizations' networks. The recent outbreak of ransomware attacks on healthcare organizations demonstrated just how vulnerable they are to the mistakes of well-intentioned employees. Compliance frameworks all require information security awareness training for employees. Many of the most publicized attacks have occurred in large organizations that presumably have access to budgets and resources for implementing the latest security technology as well as robust employee training programs. Yet, in organizations of any size, the training requirement has to compete with other resource-intensive and required processes and technology controls. Whether an enterprise is large or small, this has the natural effect of reducing investments made in training employees – the most vulnerable points on the network.

Medical identity theft continues to be on the rise as healthcare data has grown in value on the black market.

"We're a Small Fish - Who Would Target Us Anyway?"

It can be easy to think that because your organization is small or mid-sized, it can fly under the radar of hackers. This is a dangerous assumption. Thieves know that the healthcare industry generally lags behind others when it comes to protecting data. Medical identity theft continues to be on the rise as healthcare data has grown in value on the black market. That makes anyone a target. Ransomware attacks, too, do not discriminate against targets based on size. In fact, perpetrators often choose a ransom amount small enough that they know a small business can and will pay it, preferring to give in rather than risk any more downtime or compromised data.

How to Go Beyond HIPPA and Protect Your Organization

With a shift in perspective and the proper investments, healthcare organizations of any size can effectively build on their compliance programs to go beyond HIPAA and protect themselves with true security programs instead. Here's how.

Invest in a Security Program - Not Just a Compliance Checklist

If the IS team and/or management's first goal when it comes to security is "Avoid getting fined by auditors," a priority shift is in order. The first goal should be "Protect systems, customer, and employee data from a breach." Much of what is needed to be compliant will naturally follow.

We know that making this change is easier said than done. It means getting the whole organization on board – including senior leadership, whose support is required to provide the IS team with sufficient budget and resources. An important first step is to clearly communicate the value of adequate security beyond avoiding compliance violations. The risk to the business in terms of disrupted operations and lost patient trust is potentially much greater. It can only be addressed through a robust security program built over time, not by ticking requirements off of a compliance checklist.

Keep Workforce Training at the Top of Your Priority List

The real frontline when it comes to preventing or containing a security breach is your entire workforce.

The real frontline when it comes to preventing or containing a security breach is your entire workforce. According to news reports, staff training and security awareness are what helped King's Daughters' Health hospital limit the damage of a recent ransomware attack once the breach was identified[1].

Yes, proper training is a significant investment. In a busy healthcare setting, getting the time and attention of clinical and administrative staff can be especially challenging. This is also what makes good security training all the more critical. A staff member or clinician already distracted by their pressing day-to-day duties is especially at risk of mindlessly clicking on a phishing link or becoming lax about good security practices.

Too many times, we have seen the training component of the security program de-emphasized and minimally addressed in the face of bureaucratic challenges. As those who have experienced a significant breach will attest, training must remain at the top of the list.

[1] Healthcare IT News. "Two more hospitals struck by ransomware, in California and Indiana." April 4, 2016 .http://www.healthcareitnews.com/news/two-more-hospitals-struck-ransomware-california-and-indiana

Ensure that Security Processes and Procedures Take Into Account Real User Behavior

Another key to empowering your workforce on the security frontlines is ensuring that security processes and procedures are designed using a realistic and thorough understanding of people's daily workflow and behavior. Those same busy doctors and staff you've worked so hard to train may know what best security practices are, but when phones are ringing and patients are lined up in the waiting room, they can be tempted to take shortcuts. When investing in new technology and software, consider whether the solution's user experience is designed with the real-life healthcare setting in mind. It can also be valuable to ask your colleagues about challenges they may have complying with security imperatives and seek opportunities to streamline security processes and procedures.

Implement the Right Technology to Augment Limited Resources

Although people are the most important component of your security program, the proper technology is a key ally that will augment limited human resources, help your teams work more efficiently to protect data, and facilitate building and managing your IS program.

Regular vulnerability scanning is one part of effectively identifying and analyzing potential risks to electronic protected health information (e-PHI). However, because of competing priorities and resource limitations, we frequently see organizations struggling to scan often enough (if at all) or to make sense of the extensive vulnerability reports that their scanners produce.

Here's where a software-as-a-service (SaaS) vulnerability risk management (VRM) solution can augment limited resources and help you make the most out of your other security program investments. In addition to helping you demonstrate compliance, the right VRM SaaS technology will:

- Reduce staff time spent on manual VRM processes.
- Improve staff accountability, reporting, and communication to leadership and other stakeholders.
- Reduce the risk of a security breach by prioritizing vulnerabilities using context as well as intelligence and data sets beyond just the Common Vulnerability Scoring System (CVSS).
- Reduce risk through continuous monitoring.
- Improve remediation efficiency through workflow management and a unified ticketing system.

With VRM technology that is a good fit for the business, your risk of a security breach will be mitigated, and more valuable IS staff time and attention will be available for other security program components. Want to know more about reducing risk and improving business outcomes with the right VRM technology? [Download our other white paper.]

A software-as-a-service (SaaS) vulnerability risk management (VRM) solution can augment limited resources and help you make the most out of your other security program investments.

Back Up Early and Often

In the best-case scenario, you will prevent security breaches before they happen, and back-up data will never be needed. But even the most advanced and mature security programs must plan for the worst case scenario. Recent high-profile malware attacks have shown us that having access to secure backup data is the difference between continuing operations or having to turn away patients, likely losing their trust and business forever.

Prioritize backing up your most important data, especially e-PHI. Daily incremental backups, weekly full backups, and quarterly test restores are good practice in most organizations. It is critically important that e-PHI backups are encrypted in transit and at rest. In addition, ensure that frequently-needed data is stored in a place from which you can retrieve it quickly if you must. Ideally, you will also have an off-site facility for long-term data storage.

Compliance frameworks and regulatory efforts provide useful guidelines and accountability. However, simply meeting compliance requirements leaves organizations at risk. Frameworks must be customized to your organization. Leaders must understand that it takes time to mature an information security program; they must invest in the program and measure progress, rather than simply looking for a compliance checkmark. Most importantly, organizations must realize that their weakest security control is their people. They must increase the focus on and investment in their security awareness training efforts well beyond what the compliance frameworks dictate.

Add in the right technology and regular backups, and you will ensure that your organization is both compliant and safe.

Find Out How One Company Used These Tips to Mature Their Security Program

Learn how implementing the right processes and technology enabled Richard Heath & Associates to advance their security program to meet the demands of stakeholders, free up resources for other strategic initiatives, and make their organization more secure. Check out this case study (4-minute read).

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or

email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com