ipswitch®

Secure. Control. Perform.

AN IPSWITCH PROFESSIONAL GUIDE

Healthcare IT's Guide to Information Security and Compliance

ipswitch

Introduction

Ensuring healthcare IT networks are consistently compliant and secure when resources are lacking is enough to make any seasoned IT pro's skin crawl.

Your IT team likely doesn't have the time to slog through intricate checklists to meet each and every aspect of regulatory compliance. Even though your executives may be saying it's a necessary evil, you can't ever be 100% protected against a data breach.

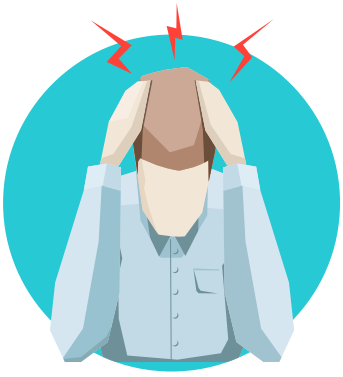
Why? Because hackers' attack vectors only become more sophisticated. Take ransomware for example. A successful ransomware attack is a data breach onto its own, quite often targeted towards healthcare organizations.

It's not a head scratcher as to why healthcare organizations are targeted. Healthcare IT networks are notoriously difficult to lock down and a hacker can make 100 times as much money off of a stolen medical record than a simple credit card.

This eBook will help you gain a better understanding of what your executives and auditors expect from you, and ways you can better protect and prepare yourself from external threats. This includes:

- Regulatory Compliance Standards and Legal Requirements
- Preparing For An Audit
- Become Ready for Anything with a Security Response Team

ipswitch



What's Your Answer?

If you are an IT pro in the healthcare industry, ask yourself and your team these questions:

- Is my organization doing everything possible to stay compliant?
- Do our users recognize when they are being phished?
- Do we have a sound plan in place to manage through a data breach?

If you answered "no" to any of those questions then you're not alone. Most organizations struggle to protect themselves from outside threats. Being compliant and ready for an audit doesn't mean you are well armed to fend off an attack from a determined hacker or disgruntled employee.

TIPS AND TRICKS

Making sure that your IT infrastructure is routinely patched to protect from the latest vulnerabilities listed is a good start for risk mitigation. We recommend you routinely check out reports from CVSS (Common Vulnerability Scoring System) and Microsoft's "Patch Tuesday" bulletins. Even with this, information security is a perpetual and thankless task. Patches alone can't promise full protection. But it's a start.

Regulatory Compliance Standards and Legal Requirements

Regulators have long been aware of the risks associated with poorly managed data transfers. Their expectations grow along with the penalties they can impose. Compliance matters everywhere, major corporations and SMBs included. These days, auditors are interpreting standards in more consistent yet more demanding ways, drawing upon a growing set of best practices. Knowing what you will get asked during an audit, before the audit happens, is your best bet.

Many healthcare and financial organizations have their own internal audit teams to prepare for outside auditors. If you are looking to create an internal group, consider staffing with a combination of experienced auditors, legal professionals, and IT managers (or some possible subset). At the very least, the internal audit team should have the knowledge and resources available to hold practice audits to identify gaps and potential weaknesses.

ISO/IEC 27001/2

Organizations are increasingly taking a closer look at the ISO/IEC 27001 international standard, widely recognized across all government and business sectors, not just in the US.

Section A.13.2 of ISO/IEC 27001 is dedicated to the subject of information transfer, with a stated objective of maintaining the security of data transferred within an organization and/or outside with external parties.

This standard is a best practice rather than a specification, and can be interpreted to suit the specific needs and risk environment of each business. Underpinning this interpretation however is a requirement to reference the more comprehensive companion standard ISO/IEC 27002.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is an international mandatory compliance requirement for all organizations processing, storing, transmitting, or accessing cardholder information for any of the major payment card brands.

The PCI DSS demands very strict security controls to be applied to protect cardholder information, including the establishment of a secure Cardholder Data Environment (CDE). The standard is enforced contractually through frequent audits and tests by approved security consultancies and vendors.

If your healthcare organization stores patients' financial data like a credit card number, you need to be PCI compliant.

General Data Protection Regulation (GDPR)

Companies storing personally identifiable information (PII) must comply with a broad range of existing information security regulations, while newer and more demanding regulations are being introduced in places like the European Union, the United States and China.

The European Commission has unified data protection regulations within the European Union under the General Data Protection Regulation (GDPR). Because GDPR is a regulation rather than a directive, it's immediately applicable to all member states. No need to panic, however, considering the GDPR does not go into full effect until May 25, 2018. Still, you can't wait until the last minute to get ready.

If GDPR wasn't enough change to manage, the UK's exit from the EU (aka "Brexit") means businesses moving and storing data in the UK will be responsible for maintaining whatever standards the UK passes, while also complying with the EU's GDPR.

GDPR goes deep, requiring privacy by design, a right to erasure, data breach notification, and data portability when a patient or customer wants a copy of their data, for example medical records. Non-compliance with the GDPR is serious considering penalties can be up to 5% of your company's annual revenue.

Health Insurance Portability and Accountability Act (HIPAA)

Healthcare organizations comply with the Health Insurance Portability and Accountability Act (HIPAA) for a bunch of reasons, like avoiding persecution from the U.S. Federal government or civil lawsuits filed by patients. HIPAA notoriously demands a wide range of administrative, physical and technical safeguards. These include formal procedures, responsibilities, training, contingency plans and internal audits to safeguard electronic protected health information (ePHI). Protected health information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Failure to comply with HIPAA can result in civil fines of up to $1.5 million per year, with criminal penalties of imprisonment for up to 10 years for deliberate violations.

Failure to comply with HIPAA can result in civil fines of up to USD 1.5 Million per year.

Preparing for an Audit

The best way to become and remain prepared for an audit is a full-on dress rehearsal. You might want to conduct your own internal audit through a certified auditor. This will help IT teams to become fully prepared as it reveals issues that need resolving. Internal audits are typically managed by members of a compliance team, including executives like your Chief Compliance Officer (CCO), Chief Security Officer (CSO), or even your CEO if it's a small business. Your compliance and security officers are often the gatekeepers for all documentation that proves your company's earnest efforts to meet compliance.

What's important to note is that in all cases of an audit, a member of the IT team will need to be present to answer any questions. This is why it is crucial to hire an internal auditor to check to see that IT has all its tracks covered before a real audit takes place. You may even want to hire a third party vendor to audit your business.

Become Ready for Anything with a Security Response Team

As regulations become more dense, data security can't be the sole responsibility of a single individual person or team. Multiple areas of the business have a stake in meeting compliance. Composing a security response team of designated compliance, security and technology practitioners including managers from all departments is a good practice. This team composition will be the most qualified to help educate users to avoid being the source of a data breach.

A WHO'S WHO LIST FOR SECURITY RESPONSE

Here is a list of people within your own organization who you should consider to take part in the formation of a security response team:

Everyone in the C-suite

All executives should be part of a security response team. A security response process can often be carved out of an existing crisis communications document. And if anyone is going to get prosecuted, it will likely be your CEO. Most senior executives are highly sought after spear phishing targets. Simply put, becoming prepared should start from the top down.

The IT Team

No surprise here that this group is very computer literate and needs to be on top of all the latest online attacks and vulnerabilities. As mentioned before, staying current with reports like CSVV, along with end user security training to teach them how to recognize social engineering tactics.

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

– HIPAA, Breach Notification Rule

Pick someone on your IT team who knows how to communicate effectively with those who are far less technical. Have that person provide a crisp and accurate representation of policy, procedures, and decisions. Much like the CEO, the CIO could be in the hot seat if there are ever legal ramifications due to a data breach.

Compliance and Security Officers

Your CCO or CSO is responsible for creating all company protocols relating to regulatory compliance. This puts them on the security response team whether or not it's what they'd chosen. They also are the gatekeepers of documentation that proves that your business has done everything necessary to stay compliant even if cybercriminals get inside your network.

Product

If you are a B2B, you most likely have a product team since you are selling products/services. The product team will have hands on experience with the technology used within an organization. Product and IT should partner up when an issue arises considering today's DevOps culture. Depending on the source of a breach or compliance point of failure, either IT or the product team will most likely be implementing a fix.

Marketing

Every security response team needs to have a seasoned corporate communications person on it. These PR experts are professional corporate crisis managers and need to control any information flow to the outside world. Many standards including HIPAA require a company that has suffered a data breach announce it via a press release if more than 500 people are affected. Smaller breaches will at the very least require some kind of notification to those affected by it.

Security and Compliance is Everyone's Responsibility

Every individual on a security response team should understand their role and responsibilities as it pertains to any given standard. Your business should have a plan in place for when an audit takes place or in the unfortunate event of a data breach.

Knowing how to respond quickly and effectively can make a world of difference on your company's balance sheet. This is why twice-yearly internal audits and practice drills are critical. Preparation is absolutely critical. There's simply no time to learn-as-you-go after you've been breached.

About Ipswitch

Today's hard-working IT teams are relied upon to manage increasing complexity and deliver near-zero downtime. Ipswitch IT and network management software helps them succeed by enabling secure control of business transactions, applications and infrastructure. Ipswitch software is powerful, flexible and easy to try, buy and use. The company's software helps teams shine by delivering 24/7 performance and security across cloud, virtual and network environments. Ipswitch Unified Infrastructure and Applications Monitoring software provides end-to-end insight, is extremely flexible and simple to deploy. The company's Information Security and Managed File Transfer solutions enable secure, automated and compliant business transactions and file transfers for millions of users. Ipswitch powers more than 150,000 networks spanning 168 countries, and is based in Lexington, Mass., with offices throughout the U.S., Europe, Asia and Latin America.

For more information, please visit www.ipswitch.com, or connect with us on LinkedIn and Twitter.

ipswitch

Download a FREE trial of MOVEit Transfer ›