Infinity Technologies

5 Tools For Passing a HIPAA & HITECH Audit at Your Office

(855) 479-4343 • www.it-va.com
4530 Plank Rd., Ste. 111, Fredericksburg, VA 22407

Table of Contents

The Evolution of Healthcare Security: HIPAA to HITECH 3

Health Insurance Portability and Accountability Act 4

Health Information Technology for Economic and Clinical Health Act 4

The Role of Audits in HIPAA and HITECH 5

1 Random Audits 5

2 Formal Audits 5

Reporting Data Breaches 6

Focusing on the Big Picture: Organizing Your Data Environment 6

Tools for Maintaining Compliance in the Modern Office 7

1 Network Health Assessment 7

2 Network Assessment Risk Report 8

3 External Vulnerability Scan 8

4 Social Engineering Penetration 8

5 PHI Data Visibility Walkthrough 9

About Infinity Technologies 10

When you signed on to run a healthcare office, you likely didn't think you'd spend your time organizing legislation and testing data security. However, the landscape of the modern healthcare office has changed. And in addition to providing excellent patient care and cutting edge medical solutions, you are also expected to capture, store, and secure the health and medical data of your patients.

It's important to educate yourself and your company on the legal requirements— and the reasoning behind the legal requirements— to make sure you protect yourself from accidental breach or attack.

In this white paper, you will find up to date information on important healthcare data legislation, as well as actionable tools and assessments you can use to ensure the highest level of protection for your company.

The Evolution of Healthcare Security: HIPAA to HITECH

When you begin operating as a healthcare organization or company that stores Protected Health Information (PHI), the following two pieces of legislation guide how you should secure and protect your company's data.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a law that establishes certain protections and requirements for consumers and healthcare organizations alike.

Title I of the law offers health insurance protection to employees and their families in the event of a layoff or job change. Protection includes access to healthcare and the portability and renewability of insurance coverage.

Title II of the law, the Administrative Simplification (AS) provision, establishes national standards for electronic healthcare information storage. The purpose of this law is to prevent healthcare fraud and abuse, simplify the administrative approach to PHI, and establish a common medical liability release.

Health Information Technology for Economic and Clinical Health Act (HITECH)

The Health Information Technology for Economic and Clinical Health Act (HITECH) is Title XIII of the American Recovery and Reinvestment Act of 2009. This section of the law allocates government funds to promote and expand the adoption of health information technology and digital storage. The result of this act is the development of Electronic Health Records (EHR) that healthcare organizations need to store and protect.

Aside from the fact that the law requires compliance, meeting HIPAA/HITECH requirements is an big step in protecting two important parties: your patients and your business.

First, these privacy requirements protect your patient's data and other Protected Health Information (PHI) from identity theft. Information contained within medical files includes passwords, social security numbers, birthdays, and security questions. All of this data can easily be used to impersonate an individual for monetary schemes such as opening new bank accounts, lines of credit and credit cards. This data can also be used for targeted phishing attempts and blackmail opportunities, which can further compromise your customer's security.

Second, these privacy requirements help protect your business from the fallout of a data breach or a random or planned audit. If you suspect or confirm that your company has experienced a data breach, you are required to self-report to HIPAA. At that time, HIPAA will audit your organization to see if you have made reasonable accommodations for the security of your patient's data. If you have not, you may be found excessively liable for the breach and face significant consequences.

The Role of Audits in HIPAA and HITECH

The main purpose of the auditing process is to make sure that your company cannot unintentionally leak data and that your office environment is set up with PHI privacy best practices in mind.

As a company that stores PHI, you may experience the following two kinds of audits:

1 Random Audits

The Office of Civil Rights' (OCR) Department of Health and Human Services (HHS) performs random HIPAA/HITECH audits to provide an extra incentive to put security measures into place. Random audits have no police involvement because they are considered to be informal events.

If you experience a random audit, HHS simply wants to look at your documentation. However, if you have no documentation, you can be sure that they will be back to perform subsequent audits.

2 Formal Audits

Formal audits are often the result of a police investigation due to a security breach. These audits involve strict requirements and guidelines that vary by state and will result in a ruling of responsibility. This ruling will affect your company's liability for a security breach and additional requirements for ongoing customer privacy and security.

As healthcare security issues continue to develop, we can expect to see influx in government involvement in the audit process as well as increased audits taking place. It's in your best interest to establish HIPAA/HITECH compliance as quickly as possible so that you are prepared when your company experiences a random audit or needs to self-report a security breach.

Reporting Data Breaches

In the event of a data breach, companies that store PHI must abide by certain requirements and restrictions. Specific requirements and timelines vary by state and the size and type of the data loss, but all states require a breach be reported as soon as it is recognized, even if it is only suspected.

Reporting a breach will not necessarily trigger an audit or an investigation, but HHS will interview your company to assess the damage or risk to your customer base. You also may be required to put out a notice to your patients via electronic communications or print media. You can find pertinent legislative requirements by state to determine what is required in your area.

Focusing on the Big Picture: Organizing Your Data Environment

Unfortunately, healthcare organizations often assume that they have the proper documentation and process in place when, in reality, they do not. You can take a quick temperature of your data environment by considering whether or not you can answer the following three questions:

1. Have you assigned a HIPAA security officer?
2. Do you have documentation for everything in your office? (Including but not limited to data storage, backup, and recovery processes.)
3. Do you have a Business Associate Agreement (BAA) with your IT services provider?

Self-auditing, assessing, and improving your data security processes may not be especially comfortable, but it will help you organize your security information and develop a mature privacy process model that protects your company's reputation and your customer's information. It will also indicate to a HIPAA/HITECH audit team that you put a reasonable amount of effort into protecting your data, which can significantly lessen your liability for breaches that do occur.

Tools for Maintaining Compliance in the Modern Office

While establishing and maintaining HIPAA/HITECH compliance can feel like an overwhelming undertaking, there are a number of resources you can use to make the process a little more manageable. Here is a list of five effective assessments that can help you root out weaknesses in your security process and identify opportunities for improvement.

1 Network Health Assessment

Infinity Technologies currently offers a free Network Health Assessment. This assessment functions as a starting point for any business that currently works with PHI or may work with PHI in the future. It's an effective way to capture an accurate picture of where your data environment stands now and how it needs to be improved in order to meet HIPAA/HITECH requirements.

In a simple and straight-forward assessment process, a Network Health Assessment reveals a variety of threats to your data security. These threats may take the form of out of date and poor performing equipment, incompetent data backups, or security gaps that could leave your network vulnerable to attack. Rather than wonder whether you are prepared to face network security threats such as malware, viruses, or malicious attacks, you can use a Network Health Assessment to capture a comprehensive assessment of what machines you have, how many you have, and what you have on them. This allows you to have a better understanding of your current situation as well as start to identify potential areas for concern that may need to be addressed.

2 Network Assessment Risk Report

A Network Assessment Risk Report begins with a straightforward evaluation of your current security process, technology, and infrastructure and points out where you might experience problems in the future. Example evaluations might include the age and condition of your servers and network infrastructure, as well as password strength and System Event Log analysis.

The risk report will also look out for unique administrative oversights such as updating and maintaining employee access for former employees and new employees. Securing the permissions settings on your computer will allow you to maintain greater control over how your machines are manipulated by both human factors and malware factors.

The result of this report will include a quantifiable Risk Score that you can use to identify an actionable plan to address each security risk and build a compliant data environment. Analyzing the results of your Network Health Assessment can also help you approach your internal security testing in the most effective way possible.

3 External Vulnerability Scan

Another option for security assessment is an External Vulnerability Scan, which is a report that provides preventative information about network points that may be vulnerable to exploitation.

During this assessment, the IT team scans available Internet Protocols (IPs) on your network to find out which ports are open and which ports are closed. They also try common passwords and combinations that hackers use to gain access to these ports and entrance to your network. The result is a deeper awareness of which ports need to be open and which do not, leading to a better understanding of how to monitor your vulnerabilities for intrusion opportunities.

Many of the DIY vulnerability scanning tools on the market, such as WireShark are complex to use, so we recommend you proceed with care. In many instances it can be more cost effective to deploy a team of experts to review your vulnerabilities and deliver a comprehensive report.

4 Social Engineering Penetration

Social Engineering Penetration is another effective kind of threat assessment tool. The process is similar to that of a traditional Secret Shopper. First, you place two fake medical records into your database. Then, a person posing as a family relative approaches your organization to try to get copies of PHI data without the appropriate identification by asking over the phone, in person, or by fax, and insisting that the person would want them to have the information.

This approach provides two important benefits to companies that handle PHI. First, it allows management to review the approval processes in place and identify gaps in employee training that need to take place before a breach actually occurs. Second, it allows employees to practice this system with fake data to prevent real threats from occurring.

5 PHI Data Visibility Walkthrough

Finally, a PHI Data Visibility Walkthrough will allow you to get a bird's eye view of the state of your physical security environment. In this assessment, IT professionals walk through your environment to see whether or not the physical security environment is adequate. They assess the physical access of the building including your security systems, what information can be seen on computer displays from different angles, screensavers, and filters, and how easy it is to capture photographs on a personal camera or smartphone as you pass by a computer. Any easily accessible PHI data signals an area that needs to be addressed.

This assessment also takes into account a variety of sources of data that may be overlooked by a DIY security protocol, such as auto logouts and lockout settings, camera systems, electronic locks, and alarms to provide a truly comprehensive view of your environment.

Both HIPAA and HITECH have physical, technological, and administrative requirements. But what's truly important is how HIPAA/HITECH affects the security of your office network and the PHI you store on your network. These laws place a significant amount of liability on your organization to organize, monitor, and protect the PHI you have. If you don't stay on top of this information, you put yourself and your patients at risk for serious breaches of data and personal security.

Your patients literally trust you with a lifetime's worth of data. Companies that take this relationship seriously understand that maintaining patient privacy and security is a vitally important process.

While protecting this amount of PHI can be a scary process, it is less scary when you have the support of seasoned HIPAA/HITECH compliance experts. Infinity Technologies has the expertise and the experience to secure your data environment against established and developing threats in the healthcare marketplace and maintain that relationship of trust and protection between you and your healthcare customers.

If you don't stay on top of this information, you put yourself and your patients at risk for serious breaches of data and personal security.

Contact us now for a HIPAA Consultation. Our HIPAA consultation covers all of the tools listed above, and will give you the information you need to secure your PHI.

Contact Us Now For A HIPAA Consultation

About Infinity Technologies

At Infinity Technologies, we understand how critical it is for our clients to protect their data and the devices that form the backbone of their business operations. Because of this, we work closely with several kinds of organizations to make sure that they have the systems in place to prevent these kinds of security threats from ever becoming a problem.

Our team of technical experts also work with our clients proactively to assess and prevent security threats on an ongoing basis. If you are looking to ensure that your company is safe from viruses, ransomware, phishing emails, or other dangerous threats that can bring your operation to a grinding halt, get in touch with us to see how we can help you meet your IT security needs and keep your office network running the way that it needs to.