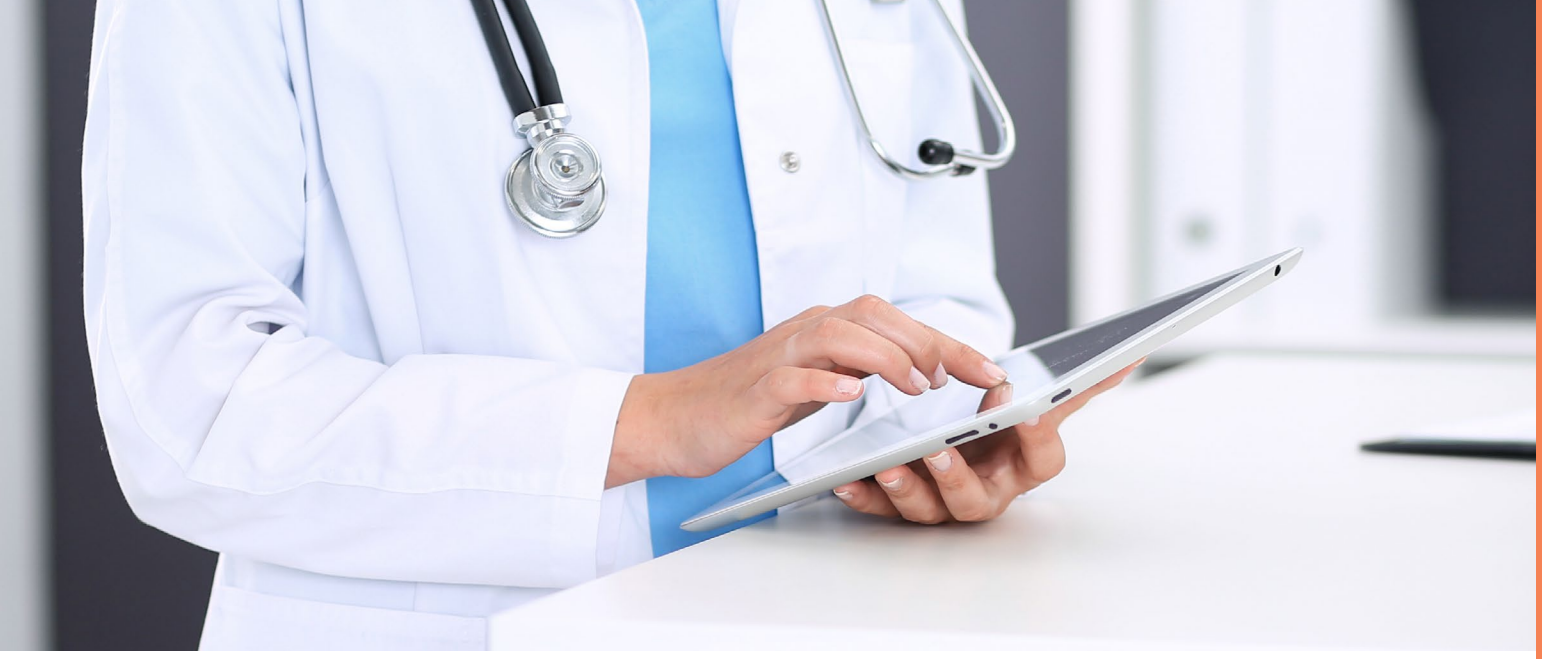
MEDICUS IT
We do 'IT' Right!

A Comprehensive Guide to HIPAA Compliance

Table of Contents

TOPIC **PAGE**

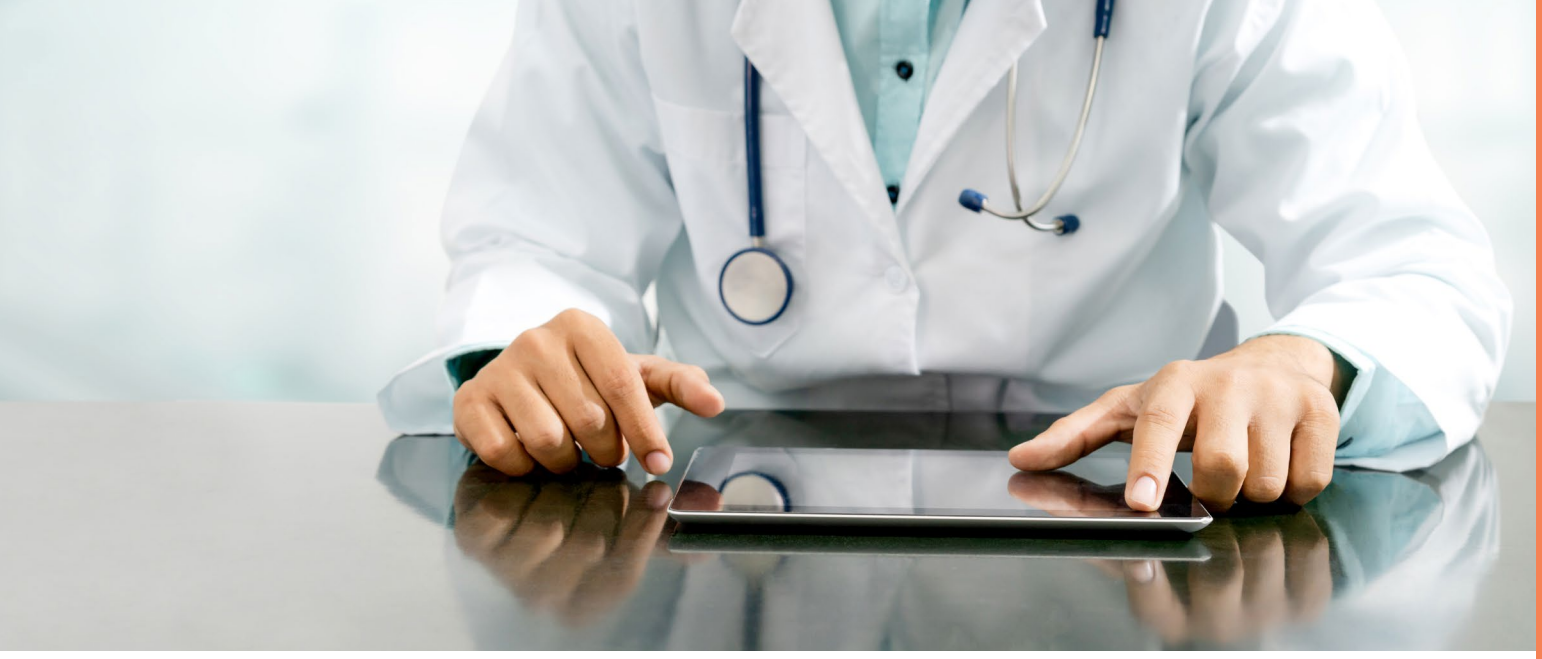


Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal statute that concerns healthcare information and insurance. While the guidelines are designed to help healthcare providers protect patient information and deliver better care, they are also dreaded by many due to their complexity and the hefty fines that can come with violations.

The cost of HIPAA non-compliance can be devastating, especially to small and medium-sized practices. It adds up quickly when you include expenses associated with government audits, violation fines, data loss, breach notifications, class-action and civil lawsuits, attorney general penalties, settlements, and corrective action plans.

At Medicus IT, we take HIPAA seriously and pride ourselves in our ability to effectively help our clients protect their data and maintain compliance. To help you better navigate the HIPAA compliance landscape, we have put together this detailed guide. It will give you an overview of some of the latest HIPAA regulations, discuss HIPAA compliance best practices, review obstacles you should be aware of and how to overcome them, and help you maximize the benefits of HIPAA compliance assessments.



CHAPTER 1: HIPAA Compliance Overview

Every healthcare provider and healthcare worker should be familiar with HIPAA regulations. But it can be overwhelming to wrap your head around the many different components. Here are some key points about HIPAA.

Top Facts About HIPAA Every Healthcare Provider Needs to Know

HIPAA offers guidelines on how to process patients' personally identifiable information (PII) for the highest level of privacy and security.

To stay compliant, you should be aware of these top facts:

1. HIPAA regulations apply to more organizations than you might think

Every organization considered a "covered entity" must ensure ongoing healthcare HIPAA compliance. The term covered entity encompasses different provider types and entities in various healthcare settings. They include physician practices, ambulatory surgery centers (ASCs), hospitals, dentists, psychologists, podiatrists, lab technicians, hospitals, clinics, nursing homes, schools with health services, nonprofits that offer healthcare services, and government agencies involved in healthcare.

A covered entity can be health insurance companies, employer-sponsored health plans, and government health programs such as Medicare and Medicaid. They may also refer to organizations that work with healthcare data (e.g., patient billing services, electronic medical records providers) or require access to healthcare information (e.g., data processing firms, medical equipment providers, law firms, and software vendors.)

2. HIPAA compliance is non-negotiable for healthcare workers

HIPAA regulations play a critical role in streamlining administrative healthcare procedures, increasing efficiency in the healthcare industry, protecting sensitive patient information, and ensuring that workers retain their healthcare insurance even if they lose their jobs. Every healthcare provider must always maintain HIPAA compliance or risk substantial fines.

HIPAA consists of 4 key components:

- **Privacy Rule:** Safeguards individuals' health information and makes sure that patients have the right to access their health records.
- **Security Rule:** Provides guidelines on how to properly store, protect, and manage electronic protected health information (ePHI.)
- **Business Associate Agreement (BAA):** Designed to ensure that any business associate (discussed further later in the guide) of a covered entity will abide by HIPAA regulations.
- **Breach Notification Rule (the Omnibus Rule):** Provides instructions on the procedures to follow in the event of a breach of unsecured protected health information (PHI).

3. Failure to comply with HIPAA regulations could cost you — a lot

HIPAA enforcement is taken very seriously. Depending on the type of HIPAA violation, providers could face fines of up to $1.5 million per year. Moreover, a failure to protect patient data can erode patient trust, cause long-term damage to the provider's reputation, and impact patient care.

4. HIPAA compliance includes technical, physical, and administrative protections

A HIPAA compliance strategy touches upon every aspect of your organization. It must cover the following:

- **Technical protections:** Encrypt and authenticate ePHI, implement access control, log changes to health data, and ensure that users are automatically logged off from the system after accessing ePHI.

- **Physical protections:** Implement a process for controlling and monitoring the personnel who can access patient data. Also, you must manage and track all the devices (e.g., laptops, smartphones, tablets) that can access PHI remotely.

- **Administration protections:** Ensure that every business associate has signed a BAA, document a contingency plan, record and track security incidents, and train staff on the latest HIPAA regulations.

5. Protected health information (PHI) has a broad definition

HIPAA focuses on protecting and managing health information that can be associated with a specific individual (i.e., patient.) PHI can include a wide range of data and must be carefully handled under HIPAA regulations. Types of patient data include:

- Patient phone numbers and email addresses
- Social security numbers
- Chart numbers
- Health insurance numbers
- Device identifiers and Internet Protocol (IP) addresses
- Biometric information, such as fingerprints or retinal scans
- Full face photographs
- Laboratory results

If the information is "de-identified" — for instance, if personal details are removed so that no specific individual can be associated with the data — then it would no longer be considered PHI and HIPAA regulations would not apply.

6. You need to perform multiple audits and document them

Maintaining healthcare HIPAA compliance is not a one-and-done process. To keep compliant with HIPAA, you are expected to conduct and document six annual audits:

- Physical site audit
- Audit of all assets and devices

- ✔ Security standards audit
- ✔ Security risk assessment
- ✔ Privacy assessment (for covered entities only, not business associates)
- ✔ HITECH Subtitle D audit

If you identify compliance gaps during these annual audits, you must document the deficiencies and create a plan to address them. You should keep all audit documentation for at least six years.

7. All staff must receive HIPAA compliance training

All staff members working in a healthcare setting must receive annual HIPAA training and security awareness training. They must understand what HIPAA is and why compliance is important. You'll need to document staff attendance and designate one employee to act as the HIPAA compliance and/or security officer.

8. Staying HIPAA compliant while working remotely can prove more difficult

The remote working trend will make it tougher to ensure HIPAA compliance. For instance, staff trained in data security on company-owned workstations may not know how to maintain the same level of protection on their laptops or other devices used outside of the workplace.

Additionally, not every employee can guarantee patient confidentiality in an at-home setting. For example, if a healthcare professional is sharing a home office with a family member, patient calls could be overheard.

To best maintain HIPAA compliance when employees are telecommuting, establish security protocols for all work devices used to access health information. Also, provide employees with HIPAA compliance training on how to set up a secure home office environment.

9. You need a detailed plan

To effectively maintain HIPAA compliance, you need a detailed plan to avoid human errors. HIPAA policies and procedures must be shared and communicated with staff members. Meanwhile, patients must also receive a notice of privacy practices that details how a provider plans to use and disclose their health information. Your policies and procedures should address information security, such as password management, data encryption, email, data backups, and data disposal.

You should define privacy policies, including how and when patient information may be discussed. Also, develop a detailed response plan for data breaches and review your policies annually to make sure they address new developments in your organization or changes in HIPAA regulations.

Once you have a handle on the main tenants of compliance, you'll want to begin strengthening your organization's HIPAA compliance performance. But before we share some guidance for you to consider, we want to discuss a concept commonly associated with HIPAA compliance that's often misunderstood: HIPAA compliance certification. Let's look at what this really means.

What You Need to Know About HIPAA Compliance Certification

HIPAA compliance certification often gets confused with HIPAA compliance, resulting in erroneous and potentially costly assumptions. There's a big difference between achieving HIPAA compliance certification and achieving HIPAA compliance. According to the *HIPAA Journal*,

> *"... there is no standard or implementation specification within HIPAA that requires covered entities or business associates to certify compliance ..."*

What does HIPAA compliance certification mean for your organization? Here's what you need to know about certification and why you may want to get certified even though it's not an essential part of achieving and maintaining compliance.

1. HIPAA compliance certification is not federally mandated

HIPAA compliance certification is not a federal requirement and does not officially provide a healthcare organization with any regulatory protections. A HIPAA certification simply means that a healthcare provider has completed training provided by a commercial third party that helps organizations become HIPAA compliant or validate existing compliance.

Receiving such certification does not mean your organization is HIPAA compliant nor "certified" by the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR,) which is responsible for enforcing the HIPAA Privacy and Security Rules. In fact, HHS does not endorse any type of HIPAA certification.

2. HIPAA compliance must be continual

There's no guarantee that an organization certified today will remain HIPAA compliant. This is one of the reasons why HHS doesn't endorse certification or offer certification itself, as explained by the *HIPAA Journal*.

There are many reasons why a practice may not remain HIPAA compliant. For example, it may adopt new technologies or experience staffing changes over time. These shifts could affect compliance, notwithstanding changes to the HIPAA regulations.

3. Employee training is essential for HIPAA compliance

While the HIPAA regulations do not mandate any specific training program, they do have workforce training and management requirements:

> *"Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity.) A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the (HIPAA) Privacy Rule."*

Meeting these requirements is a lot of work, and many healthcare organizations outsource the training and education on HIPAA for their staff. Some healthcare providers seek certification to facilitate staff training, even though HIPAA certification provides no special protection when it comes to compliance audits. This is because:

> *"performance of a 'certification' by an external organization does not preclude HHS from subsequently finding a security violation."*

4. Do your due diligence when pursuing HIPAA compliance certification

If you decide that HIPAA certification is right for your healthcare organization, take the time to evaluate your options. Look for a certification process that delivers tangible benefits and not just a certificate to post on your website. Companies offering certification have different approaches, and most of them begin the process by conducting a HIPAA assessment to identify potential vulnerabilities and weaknesses. Then, they'll assist you with implementing fixes and improvements. Employee training and a review of policies and procedures may also be part of the package.

Keep in mind that some health IT experts question whether certification is worthwhile. Instead of spending in-house resources to achieve an unrecognized certification, it may make more sense to outsource your healthcare information security needs to a reputable health IT service provider that is well-versed in HIPAA compliance, keeps current on changes and developments, and can demonstrate a track record of success.

CHAPTER 2: HIPAA Compliance Best Practices

Bringing your healthcare organization into compliance with HIPAA is just the first step. The challenge is to then remain compliant as regulations evolve and your organization undergoes changes over time.

To adapt to these changes, you need to understand the purposes of HIPAA, which include the following:

- Ensure protection and confidential handling of PHI
- Reduce the likelihood of healthcare fraud or abuse
- Mandate industry-wide standards for healthcare information contained in electronic billing and other processes
- Provide the ability to transfer and continue online health insurance coverage for patients when they change or lose their jobs.

Staying Current with HIPAA Compliance Requirements

New circumstances often present obstacles to staying compliant with HIPAA regulations. Let's examine some common challenges and how to overcome them using ongoing best practices that can help you stay current now and in the future.

Problem: New technologies or procedures are introduced that disrupt compliance.
Solution: Conduct risk assessments

Conduct a HIPAA risk assessment annually to help your organization maintain ongoing compliance. A risk assessment may be required more than once per year if new technologies or procedures are introduced. *HIPAA Journal* recommends that a risk assessment should cover the following:

- ✔ Identify where PHI is stored, received, maintained, or transmitted
- ✔ Identify and document potential threats and vulnerabilities
- ✔ Assess current security measures used to safeguard PHI
- ✔ Assess whether the current security measures are used properly
- ✔ Determine the likelihood of a "reasonably anticipated" threat
- ✔ Determine the potential impact of a breach of PHI
- ✔ Assign risk levels for vulnerability and impact combinations
- ✔ Document the assessment and act where necessary

Conducting a risk assessment can be challenging for small or medium-sized practices. To better ensure a thorough assessment, work with an experienced healthcare IT professional so you can be confident that any HIPAA compliance issues and vulnerabilities are uncovered and addressed.

Problem: Protected health information (PHI) is stored in multiple places
Solution: Identify and analyze the location of PHI and all systems that may contain it

A protected health information analysis evaluates every element of PHI within your organization and its information systems. While the HIPAA Security Rule covers ePHI, you should also take inventory of all data stored on paper. This will help reveal risks that should be addressed so you can better secure all information from potential breaches. Your practice's PHI should be reviewed at least annually.

While identifying how information is collected, used, stored, shared, and disposed of can be straightforward, protecting such data isn't as simple. Consider partnering with a healthcare IT specialist to perform a thorough PHI analysis and ensure that your PHI is secure.

Problem: Staff, services, technology changes can make policies ineffective if they are not updated

Solution: Frequently develop and implement documented standards for your policies and procedures

At least every two years, or more frequently if your organization undergoes significant changes, your policies and procedures should be reviewed and updated. By developing and implementing policies and procedures, you communicate to staff and patients that roles and responsibilities have been established to keep PHI secure. This also enables you to explain how you'd handle an incident such as a data breach.

Policies your practice should have in place include the following:

- **Security policies —** These may include procedures designed to protect PHI, such as password management, encryption, email, data backups, device disposal, and more.
- **Privacy policies —** These should include rules that pertain to how patient information is shared within your organization and with third parties.
- **Breach notification policies —** These detail the rules or steps your organization must take if a data breach occurs. You should include a current incident response plan (IRP,) which outlines guidelines related to PHI security-related incidents that meet HIPAA requirements.
- **Procedures —** These are necessary steps that staff must follow to implement your policy. For example, explain how employees should utilize healthcare IT software to keep patient information secure.

You can partner with a healthcare IT specialist to ensure that you meet all requirements for the EHR Incentive Program and annual HIPAA security risk analysis (SRA), so you can put your organization in a position to receive financial incentives that support your compliance efforts. Yet, there are more steps you can take — starting with reforming as many paper-based processes as possible.

Why You Should Implement HIPAA-Compliant Electronic Forms

The migration from paper-based to electronic HIPAA compliance forms has become increasingly important to achieving and maintaining HIPAA compliance. Consider the following:

- The Health Information Technology for Economic and Clinical Health (HITECH) Act incentivizes healthcare organizations to use electronic health records to increase efficiency and portability. It also permits the OCR to audit and punish non-compliance more aggressively.

- The HIPAA Omnibus Rule specified a patient's right to electronic PHI, broadened the definition of business associates with whom healthcare organizations must maintain HIPAA agreements, and required updates to notice of privacy practices (NPPs.)

- Plans are under consideration to enhance patient access to PHI, boost information-sharing, and improve case management across the care continuum.

What do these all mean to healthcare providers? It's imperative to be able to share your HIPAA compliance forms (e.g., NPP, authorizations, intake records, BAAs) quickly and store them in a controlled way. This means switching to electronic forms.

Below are some of the common problems that switching to electronic HIPAA-compliant forms helps to address.

1. Administrative tasks need to be consolidated

When records are maintained in different formats (e.g., paper, discs, faxed, hand-filled requests), management and organization become more difficult, bringing elevated risk. Consolidating all forms and documents onto an electronic system can help limit liability. Use e-forms to manage NNP receipt with e-signature, BAAs, patient authorizations, intake and health insurance information, and other documents containing sensitive patient information. Electronic forms can also help lighten administrative burden since they can be easily searched, reorganized, and deleted.

2. Form loss poses a significant risk

When handling patient forms, you must consider the following:

- Have new patients consented to share their PHI as detailed in the NPP? If they neglected to sign, was it recorded that they saw the notice? An e-form can keep track of this process.

- Did a patient fill out all necessary information, so duplicates do not need to be created and re-filed? E-forms can better ensure that patients provide required information before submission.

- Was a new BAA mailed or faxed? Is someone keeping up with its status? E-forms can help you track all the proper steps.

Keep in mind that the benefits of using e-forms won't be realized unless all your forms are digitized and kept uniformly, allowing you to leverage software and standardized workflows to improve accuracy.

3. Paper-based forms are not easily portable

Healthcare providers can be punished for not processing releases and making PHI available upon request. In fact, the first monetary penalty issued by the OCR in 2011 was a $4.3 million fine to a Maryland entity for denying 43 patients timely access to their medical records and refusing to cooperate in the investigation.

With proposals aiming to shorten the 30-day limit for delivering PHI to patients, speed for transfer is likely to become even more imperative in the future. Electronic forms are the key to strengthening improving patient accessibility demanded by HIPAA legislation.

4. Paper-based forms do not have built-in tracking or protection

Electronic HIPAA compliance forms make it easier to prevent breaches by controlling access to information, requiring authentication, and producing login records. The use of electronic forms also mitigates human errors associated with paper forms.

Breaches have many causes, some of which may be out of your control. After all, cybercriminals have sophisticated and ever-evolving attack methods. Nonetheless, the better your forms and PHI are monitored, the more likely you can catch a breach, report the breach to OCR, and address it before cybercriminals can cause significant damages.

Even after switching to electronic HIPAA-compliant forms, there are other important considerations for protecting data. For instance, you'll want to consider what the lifecycle of digital information looks like. At some point, data stored on hardware must be discarded. If any of that data contains sensitive patient information, there are rules you'll need to know and follow before proceeding.

How to Maintain HIPAA IT Compliance When Disposing of Hardware

Data breaches caused by the incorrect disposal of hardware that contains PHI are a risk that healthcare providers cannot afford to overlook. HIPAA IT compliance requires that any PHI your organization stores on electronic devices must be disposed of according to specific guidelines. Follow these steps to better protect data stored on electronic devices and media.

Identify devices with PHI

First, conduct a full risk analysis of your organization's IT infrastructure and evaluate administrative, physical, and technical safeguards. A healthcare-focused IT firm can create an inventory of all your organization's electronic devices that may contain PHI to determine the best ways to dispose of them. At a minimum, you should include the following devices on your disposal list:

- ✔ Desktop computers
- ✔ Laptops
- ✔ Servers
- ✔ Tablets
- ✔ Mobile phones
- ✔ Portable hard drives
- ✔ USB drives
- ✔ Zip drives
- ✔ CDs, DVDs, and backup tapes

Additionally, some devices may store patient data on internal hard drives. They can include x-ray machines, fax machines, pacemakers, defibrillators, CT and MRI machines, copiers, and printers.

Properly dispose of hardware with PHI

When it's time to dispose of hardware that contains PHI, how can your organization do so while staying HIPAA compliant? While there is no one preferred method, healthcare providers must follow regulations established by HHS and then develop a plan and procedures specific to your organization's hardware and data storage processes.

According to HHS, any devices with PHI cannot be disposed of in a dumpster that's accessible by the public. One exception is if the PHI:

> *"... has been rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster."*

The HIPAA Privacy and Security Rules have several disposal requirements that organizations must follow, such as the following:

- **PHI on electronic media —** Consistent with NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, HIPAA regulations require devices to be cleared (using software or hardware products to overwrite media with non-sensitive data,) purged (degaussing or exposing the media to a strong magnetic field to disrupt the recorded magnetic domains,) or destroyed (disintegration, pulverization, melting, incinerating, or shredding) before disposal. Asset tags and corporate identifying marks should also be removed.

- **Depositing devices containing PHI in locked dumpsters —** Devices containing PHI must be disposed of in dumpsters that are only accessible by authorized persons, such as appropriate refuse workers.

- **Business associate agreement for third-party contractors —** If your organization chooses to work with a third party to dispose of electronic devices that contain PHI, you must enter a BAA with the vendor before work begins. Anyone who may handle these devices should be aware of their responsibilities concerning the proper disposal of these items.

- **Physical security controls —** Processes should be in place to ensure devices cannot be stolen or accessed by unauthorized individuals. Such security controls include the safe transportation of devices until all data is destroyed.

Train staff on proper device disposal

Educate your staff on how to properly dispose of hardware. Every healthcare provider is different, so training should be customized to suit your needs. Here are a few recommendations to get started:

- Training should include staff members who are directly disposing of PHI and anyone who supervises these employees.

- Your HIPAA compliance training, which is typically conducted annually, should include information about the proper disposal of hardware. Provide this training soon after new staff members are hired to avoid mistakes that could jeopardize compliance.

- Your organization's training should cover all devices that may contain PHI as well as the policies and procedures that are in place to properly dispose of these devices.

- Staff should know if your organization has a secure depository where hardware should be placed while it awaits disposal.

How long should you keep devices containing PHI?

According to the HIPAA Security Rule, you should keep PHI and devices containing such data for at least six years, though different states may have rules that require you to keep them longer.

Also, the HIPAA Privacy Rule states that organizations must

> *"... apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other PHI for whatever period such information is maintained by a covered entity, including through disposal."*

Penalties and risks for improper disposal

If devices are not disposed of correctly, your organization can face potential fines. These penalties, along with the associated risks and expenses, are likely to get much worse if a data breach occurs. Penalties can include the following:

- Besides notifying all affected patients, your organization may need to pay for credit monitoring, identity theft protection, legal counsel, and more for these individuals.
- Patients whose data was exposed may file a lawsuit, and you may have to pay a settlement along with legal fees.
- Investigations may be conducted, which can result in significant financial expenses. You may incur HIPAA fines and penalties if you haven't implemented the appropriate safeguards for devices that contain PHI. An organization may be fined thousands to millions of dollars depending on the severity of a breach.

Since HIPAA training requirements are complex, including those concerning the disposal of hardware, many healthcare providers choose to partner with a healthcare IT specialist to ensure that staff receives timely and current compliance information from experts in HIPAA IT compliance.

Not all obstacles to HIPAA compliance are apparent, which is why it's necessary to take proactive measures to help identify potential shortcomings. That's one of the reasons HIPAA compliance audits are required.

Preparing for a HIPAA Compliance Audit: Security Risk Assessments (SRA)

Now you know the value of implementing HIPAA compliance best practices. But with so many moving parts, where should you begin?

The first step is to take inventory of your IT infrastructure and understand potential vulnerabilities by conducting a HIPAA security assessment, also referred to as an SRA (security risk assessment). Such an assessment, often provided by a third party, will help you identify and address potential violations of HIPAA regulations.

The primary purpose of a HIPAA compliance audit is to ensure that patient data is secure and protected at all levels within a healthcare organization. Auditors will evaluate your progress on achieving compliance and identify areas where improvement is needed. An SRA can also help you better prepare for a HIPAA compliance audit administered by the federal government. Here's what you can expect from an SRA.

1. Identify vulnerabilities before they become serious issues

HIPAA guidelines require every covered entity and business associated to:

> *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity."*

A thorough security risk assessment is more than just a nice to have. Instead, it is a regulatory requirement.

Security assessments aren't just a checkbox exercise. They can help you build and maintain the systems and processes needed to protect your PHI. The assessment will review every aspect of your operations, IT systems, hardware, processes, staff security training, and more. It will identify vulnerabilities before they turn into serious issues so you can either resolve them or monitor them carefully.

2. Build a complete and well-documented history of data security measures

During your security risk assessment, the third-party assessor should review the following areas:

- ✔ PHI storage, maintenance, and transmission
- ✔ Potential threats and vulnerabilities
- ✔ Current security measures
- ✔ Correct usage of security measures

- Likelihood of threats to patient data safety
- Potential impact of a data breach
- Level of the vulnerability of your various IT systems and data management processes
- Need for future action
- Need for further staff training

The SRA should provide you with extensive documentation of all these areas and an action plan to address existing vulnerabilities. Such complete documentation can also help you pass your HIPAA compliance audit with flying colors.

3. Provide detailed insights into your entire patient data management structure

It can be all too easy to miss some essential facets of patient data security in a busy healthcare organization. A thorough security risk assessment will help uncover these shortfalls. Your risk assessment should examine the following:

- Access to wireless services
- Digital data storage devices
- Physical data storage
- Physical access to confidential information
- Printers and copiers
- Email, fax, and phone systems
- Portable device security
- Computer security
- Firewalls
- Medical device data systems
- Electronic health record (EHR) systems

- ✔ Website forms
- ✔ Retired and decommissioned data storage systems

A comprehensive HIPAA security risk assessment will examine and identify potential risks across your entire IT operation, giving you a clear picture of how patient data is handled from end to end to better ensure that you're prepared for a HIPAA compliance audit.

4. Keep your data security measures current

A HIPAA risk assessment is not a one-time exercise. Rather, assessments should be performed regularly to track your progress in achieving compliance and addressing issues. Every time you implement a significant new work practice or introduce new technologies, you should conduct a security risk assessment to identify potential risk areas and build a training plan to make sure the tools are used in a HIPAA-compliant manner.

By following such best practices, you can reduce the likelihood of being caught off-guard by outdated security measures or a lack of current documentation.

To help ensure readiness, some companies find value in using checklist tools. Let's explore the benefits of this approach.

Why Your Organization Should Use a HIPAA Compliance Checklist

HIPAA compliance involves the continuous monitoring of technical, physical, and administrative processes. Failure to comply with HIPAA regulations can result in massive fines and lasting damages to your organization's reputation.

Fortunately, there's a straightforward and low-cost solution to keep your organization HIPAA compliant: a HIPAA compliance checklist. This resource can be as simple as a list with checkboxes, either in a digital or paper format, to cover areas of HIPAA compliance and identify required actions that your employees must complete to ensure compliance.

Here are seven reasons why your organization should leverage a HIPAA compliance checklist.

1. Checklists work incredibly well in high-stakes situations

Checklists are highly effective at reducing memory-related errors, particularly when people are active, under time pressure, and in stressful situations. That's why checklists

are frequently used for surgery and intensive care. You can adopt this method to help enforce HIPAA compliance as well.

2. Checklists create clarity

The process of creating, reviewing, updating, and completing a HIPAA compliance checklist helps prevent your team from overlooking critical areas. This systematic approach to risk management better enables you to detect threats to and vulnerabilities within your organization that could result in the unauthorized disclosure of PHI. By addressing vulnerabilities, you can avoid potential damages to your brand and patient trust while reducing the risk of breaching HIPAA guidelines and incurring hefty fines.

3. Checklists facilitate knowledge management

HIPAA requires covered entities to assign an employee as HIPAA compliance officer. This individual is responsible for ensuring HIPAA compliance in your organization. However, if that person is unavailable for the short or long term, HIPAA requirements might be overlooked. A checklist helps maintain consistency when there is a transfer of responsibility from one HIPAA officer to another.

4. Checklists help you prioritize

A HIPAA compliance checklist gives you visibility into issues of concern. It also helps you create and document a plan to address these challenges, as required by HIPAA. Such a level of transparency also allows you to prioritize the issues according to their risk level.

5. Checklists help you build a culture of compliance

Becoming a HIPAA-compliant healthcare provider isn't just a question of box-ticking. To maintain compliance over time, you need to create a HIPAA-aware culture. That way, if employees change a process or update a system, they'd know to check for compliance issues or inform the HIPAA officer without being reminded.

As a simple risk management tool, checklists help effectively communicate with employees about your security priorities. Once you have a working checklist in place, make sure every employee who works with PHI receives a copy. You can introduce the checklist in a workshop to help ensure that everyone understands how to implement the procedure.

6. Checklists can improve compliance training

Checklists can help you create more effective HIPAA training programs, which you must provide to comply with HIPAA. By working through a HIPAA compliance checklist and

reviewing best practices, you can create a customized training course that is much more likely to result in positive outcomes.

Training your employees in compliance best practices is far better than correcting bad practices in the workplace randomly as you see them happen. Being proactive is not only the right thing to do but can also greatly reduce the risk for your organization.

7. Checklists support compliance documentation

The documents used in creating a HIPAA compliance checklist also satisfy some of the administrative safeguards mandated by the HIPAA Security Rule. Aside from advancing your compliance efforts, the documents may aid an investigation process and reduce your costs if your organization experiences a breach or is selected for a HIPAA audit.

How To Create a HIPAA Compliance Checklist

The HHS does not provide a standardized HIPAA compliance checklist because no two organizations face the same HIPAA compliance risks. Checklists should be designed specific to an organization's operations and needs.

To create a HIPAA compliance checklist, it's best to partner with a consultancy or managed services provider (such as Medicus IT) with HIPAA expertise or work with an experienced HIPAA officer.

Begin by conducting a systematic HIPAA risk assessment to identify critical infrastructure vulnerabilities that can put PHI at risk. From there, review each of the potential risk areas and create a plan to address them. Finally, create a customized checklist for your organization by considering a broad range of compliance areas such as:

- ✔ Annual audits and assessments
- ✔ Business associates
- ✔ Contingency planning
- ✔ Data encryption
- ✔ Documentation
- ✔ Identity management
- ✔ Patient access

- ✔ Policies and procedures
- ✔ Training
- ✔ Updates and changes to systems and operations

We strongly believe in the value of using a HIPAA compliance checklist. As such, we have created a HIPAA SRA checklist template, which you can download here to jumpstart your effort.

Even with the best-laid plans, cybercriminals can still potentially exploit holes in your security posture. That's why it's a good idea to consider what the threat landscape looks like and what your organization can do in response.

CHAPTER 3: HIPAA Compliance Obstacles to Success

Cybercrime is a billion-dollar black market, and the healthcare industry is a prime target. It's been among the most popular for cybercrime in recent years. Staying on top of the latest cybersecurity best practices and changes in HIPAA legislation can be challenging. Yet, healthcare organizations can't afford to have compliance gaps that can be exploited by cybercriminals.

It's therefore critical to understand the most significant threats to HIPAA cybersecurity compliance and healthcare systems. Below are some common HIPAA cybersecurity threats and obstacles to HIPAA compliance success. They show how organizations may go awry with compliance and how you can put in the necessary measures to better keep your organization protected.

1. Phishing, Malware, and Ransomware

Phishing is one of the top causes of data breaches. Simple in concept, phishing schemes rely on gaining key information by fooling unsuspecting employees into doing something via email (e.g., downloading malware or clicking on a malicious link.) The goal is to infiltrate an IT system.

Many phishing schemes are designed to deliver malware, which can hide in downloads. Malware can include viruses, trojans, adware, spyware, ransomware, and other malicious programs. It can remain largely hidden to collect information or lock up an entire system. In 2015, the University of Washington School of Medicine was fined $750,000 after 90,000 patient

records were potentially exposed in a phishing incident. One employee opened a likely-forged email to review a document that looked reputable. This misstep resulted in fines, public reputation damage, and the expense of corrective actions.

Ransomware is a type of malware that's a growing threat. Ransomware encrypts important files and systems so an organization cannot access and use them. This can slow down essential processes or render them inoperable. Once files are encrypted, cybercriminals typically demand payment in cryptocurrency to release the files. However, there is no assurance that the criminals will release the files after payment is made.

Here are four strategies to increase resilience to phishing and malware you should add to your HIPAA cybersecurity program:

- **Minimize available information about employees —** Public directories and other documents with details about staff members are often used for phishing. The more information available about a person, the more convincing (i.e., personal) phishing emails can be.
- **Train employees on cyber incidents —** Employees should regularly be drilled with phishing simulations and learn about how real-life successful attacks occurred. Those exposed to simulations had a median click rate 25% lower than those who did not.
- **Filter out suspicious content —** All email systems should have filtering mechanisms to block phishing attempts by quarantining suspicious inbound messages and blacklisting phishing sources.
- **Multi-factor authentication (MFA) —** Cybercriminals often try to exploit usernames and passwords to access networks. Reduce vulnerability by implementing another level of security to confirm the identity of a user. It could be a security question, PIN, or a registered device that interacts with the computer.

2. Legacy Systems

A legacy system is an outdated system no longer actively patched and maintained. Its vulnerabilities can become well-known. Cybercriminals are more likely to infiltrate a network through outdated programs. Yet, many healthcare providers still use legacy systems because of the expense and administrative disruption that they believe an overhaul can cause. Surveys have shown that many individuals and business using legacy systems. One of the most common is Windows 7, which was added to the list of obsolete software as of January 2020.

It is critical to determine what legacy systems are still in use by your organization and devise a plan to perform necessary upgrades or replacements.

3. Insufficient Employee Training

Although your employees may be aware of common phishing scams, there are other avenues through which breaches can occur. Whether it's caused by intentional misconduct or, more commonly, a lack of awareness, employee behaviors should be at the top of your list of concerns and a significant focus of your HIPAA cybersecurity checklist and training. *HIPAA Journal* identifies these common ways that poor employee practices may be putting PHI at risk:

- **Snooping on medical records** — Healthcare employees who have received HIPAA training should understand what is considered a violation of their employer's HIPAA policies. Yet, this is not always the case: From 2012 to 2020, Kaiser Foundation Health Plan of the Mid-Atlantic reported an employee inappropriately accessed members' radiology records. Lurie Children's Hospital of Chicago reported an employee inappropriately viewed more than 4,800 patient medical records.

- **Mishandling of PHI** — This broad category can include everything from insufficient PHI access controls and emailing PHI to personal email accounts to downloading PHI onto unauthorized devices. Cited as one of the 10 most common reasons for HIPAA violations, using unauthorized devices is often a shortcut for time-crunched staff. But HIPAA security rules clearly state that:

> *"Clinicians and team members working virtually may access PHI only on authorized devices and must avoid downloading them to unsecure locations."*

Proper training must emphasize this rule, as well as the one that requires covered entities and their business associates to limit access to PHI to authorized individuals. The failure to implement appropriate ePHI access controls is also one of the most common HIPAA violations and has garnered a lot of attention. For instance, *HIPAA Journal* cites the example of Anthem, which paid $16 million in fines for access control failures and other HIPAA violations.

- **Improper disposal of PHI** — Training your employees on how to securely and permanently destroy PHI is essential. As *HIPAA Journal* states,

> *"For paper records, this could involve shredding or pulping and for ePHI, degaussing, securely wiping, or destroying the electronic devices on which the ePHI is stored to prevent impermissible disclosures."*

It might seem simple, but as recently as 2019, *Becker's Hospital Review* reported that seven healthcare providers disclosed that patient and employee records were dumped in unsecure locations.

4. Non-Compliant Third-Party Business Agreements

You could risk a HIPAA violation if you engage with third-party vendors and business associates whose work involves handling sensitive data but are non-compliant with HIPAA rules. Even when business associate agreements (BAAs) are in place for your partners, they may not be HIPAA compliant or continually assessing their risks.

Healthcare providers must do their best to verify that any partners responsible for managing PHI follow HIPAA policies and procedures. Regularly reviewing and updating business associate agreements should be an item on your HIPAA cybersecurity checklist.

5. Loss or Theft of Technology

Loose security standards can put your organization at risk of theft. Even if theft cannot be proven, the inability to account for records represents an equal risk.

6. Failure to Use Encryption on Portable Devices

Although encryption is not a requirement, it's a HIPAA cybersecurity best practice for defending against threats. According to *HIPAA Journal*,

> *"Breaches of encrypted PHI are not reportable security incidents unless the key to decrypt data is also stolen."*

When weighing whether to implement encryption, consider the cost implications of not adding this safeguard. In 2017, the Children's Medical Center of Dallas received a $3.2 million civil monetary penalty for

> *"failing to take action to address known risks, including the failure to use encryption on portable devices."*

7. Impermissible Disclosures of PHI

Any disclosure of protected health information not permitted under the HIPAA Privacy Rule can result in a financial penalty. OCR reports that it has investigated and resolved more than 28,000 cases by

> *"requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA-covered entities and their business associates."*

The investigation yielded some important insights. For example, the report states that among the compliance issues most often alleged in complaints, "impermissible uses and disclosures of protected health information" tops the list in terms of frequency.

The impact of overlooking this issue could have staggering consequences. The OCR reports that it has settled or imposed a civil money penalty in close to 100 cases resulting in a total dollar amount of more than $135 million.

8. Improper Use of Electronic Forms

HITECH recommends that healthcare providers use electronic health records to increase efficiency and portability while better ensuring HIPAA compliance. Proposed rules that aim to enhance patient access to PHI, boost information-sharing, and improve case management across the care continuum are making the digitalization of PHI even more urgent.

Healthcare organizations often make the mistake of using a mix of paper and e-forms. This can result in information being stored in different places and make compliance even more challenging. Additionally, not using the right software or workflows to manage e-forms can make an organization more volume and increase opportunities for hackers to access PHI.

Lastly, don't overlook the importance of identifying and protecting remote access points from cyberattacks as you migrate PHI to digital format. You can read more about how to strengthen remote access security and ensure patient confidentiality here.

9. Improper Disposal of Devices

Devices on which PHI is stored must be disposed of properly or you could risk having the information stolen by malicious actors. Here are some common mistakes to avoid in this area:

- **Neglect to train home healthcare workers —** If your organization employs home healthcare workers, they must know how to securely dispose of devices that may store PHI. While there isn't a specified way for home healthcare workers to dispose of hardware, they should be trained with the rest of your staff and consistently follow your organization's policies.
- **Reusing hardware with PHI —** Another area that organizations may overlook is the reuse of hardware that previously used to store ePHI. Don't forget to properly dispose of PHI stored in the devices before reusing them.
- **Only performing simple deletion of data —** Some organizations may think that deleting all the data or formatting the hard drive before disposal is enough. But if you fail to clear

data thoroughly, traces could be left behind. Some criminals may even be able to retrieve the data, putting your organization and patients at risk. It's critical to have the appropriate procedures in place to purge data and verify that it has been completed deleted.

10. Not Using a HIPAA-Compliant Phone Service

HIPAA regulations apply to all forms of patient communication, including phone calls, voice messaging, text messages, call recording, and video calls. If you communicate with your patients via phone, you must use a HIPAA-compliant phone service.

Your phone service must satisfy the conditions specified in the HIPAA rules. In particular, your VoIP vendor must offer features including:

- ✔ Encryption for all stored data, including call recordings and chat logs
- ✔ Detailed call records
- ✔ A unique ID for every phone in the system, each with a specific username and password
- ✔ Role-based access controls

A HIPAA-compliant phone service helps you stay compliant, protect patient information, ensure a secure IT system, support a remote workforce, and facilitate the shift to telehealth services.

11. Not Conducting Regular and Professional Risk Assessments

If you are found to have violated HIPAA regulations during a compliance audit, you may face a significant fine. As the *HIPAA Journal* notes,

> *"More recently, the majority of fines have been under the 'Willful Neglect' HIPAA violation category, where organizations knew — or should have known — they had a responsibility to safeguard their patients´ personal information. Many of the largest fines — including the record $5.5 million fine issued against the Advocate Health Care Network — are attributable to organizations failing to identify where risks to the integrity of PHI existed."*

Healthcare organizations that fail to ensure the safety and integrity of their patients' PHI are putting their organization, financial stability, and patients' data at risk. HIPAA security risk assessments should always be performed by a qualified third party with healthcare experience and expertise. Even if you have your own in-house IT team, it's best to work with an experienced healthcare IT firm for your risk assessments.

Why? An IT firm that specializes in HIPAA compliance will be more likely to identify shortcomings. With an unbiased and objective viewpoint, they are better positioned to catch overlooked problems and deficient processes. As the saying goes, you don't know what you don't know. Not to mention, regular and comprehensive risk assessments can help you identify many of the pitfalls we discuss here, so you can prevent them from festering into costly issues.

With all of that said, the effectiveness of these assessments will depend heavily on how your company chooses to optimize their usefulness.

Chapter 4: Maximizing the Value of HIPAA Compliance Assessments

Violating HIPAA regulations can have serious consequences for organizations and patients. A proper HIPAA risk assessment is crucial to complying with security standards and achieving compliance.

Why a HIPAA Risk Assessment is Critical to Achieving Compliance

A HIPAA risk assessment provides an accurate and thorough evaluation of the potential risks and vulnerabilities to protected health information in your organization. In fact, it must be conducted whenever certified EHR technology is adopted in the first reporting year.

Here's the critical role that a risk assessment plays in helping ensure compliance.

Importance of a HIPAA Security Assessment

A HIPAA risk assessment is vital for identifying and addressing issues concerning confidentiality, integrity, and availability of PHI. The HIPAA security assessment pinpoints shortcomings, so healthcare providers can take appropriate actions, implement improvements, and mitigate such risks through physical, technical, and organizational safeguards.

Healthcare providers should take the HIPAA risk assessment seriously — not only because of its role in helping safeguard PHI but also to avoid penalties. Security risk assessment (SRA) failures are a common precursor for HIPAA penalties. Many OCR HIPAA settlement actions concerning electronic PHI breaches involve insufficient risk analysis. Healthcare providers that struggle with risk assessment should seek professional help to identify and address vulnerabilities and avoid penalties.

Understanding HIPAA Security Assessments Rules

Performing a risk analysis regularly is an integral part of a solid action plan for protecting PHI. The HIPAA Security Rule, section 164.308(a)(1)(ii)(A) states that a risk analysis is required. Specifically, the Guidance on Risk Analysis states that every organization must "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

Acquiring written proof of compliance by conducting a risk analysis does more than fulfil a requirement. It identifies vulnerabilities in the security of your organization, so you can strengthen security and better protect patient information. Without a risk analysis, weak points could go unnoticed. They may worsen over time, putting your patients' privacy and your organization in even greater jeopardy.

How HIPAA Security Assessments Help Ensure Compliance

The HIPAA security assessment is a complete audit of all your healthcare organization's systems, processes, hardware, and more. It analyzes every nook and cranny of your infrastructure.

A well-formed and executed HIPAA risk assessment will find problems and vulnerabilities. Once you identify the areas that need addressing, they can be fixed or monitored. You are less likely to encounter unpleasant surprises if your organization undergoes a HIPAA audit.

The preventative nature of an SRA allows you to identify vulnerable systems before problems arise to avoid fines. It is important to note that SRAs will only help improve compliance if executed correctly.

How to Conduct a Proper HIPAA Security Assessment

HIPAA risk assessments can be very effective — when done thoroughly. Assessments are intended to essentially examine every inch of your infrastructure, so the process can feel arduous. How can you make sure the job is done right? The Office of the National Coordinator for Health Information Technology (ONC) offers a few resources to streamline the process, one of which is a security risk assessment tool.

This tool guides small companies through the HIPAA security assessment process. When you enter information into the SRA Tool, data is stored locally on your device. HHS doesn't receive or access your data in any way, so you don't have to worry about data security.

After completing the assessment, you'll receive a results report. You can use it as a guide to locate risks and strengthen policies, processes, systems, and methods that require attention. The SRA Tool undergoes periodic updates, including one in September 2020. New features are intended to make the new SRA Tool easier to navigate while delivering a more in-depth risk assessment. Expanded exporting capabilities make reports easier to share.

A More Reliable HIPAA Security Assessment Method

While the SRA Tool can be a helpful resource, it has some shortcomings. The federal government notes that the SRA Tool

> *"... is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks."*

The target audience of the tool is smaller organizations (with 1-10 healthcare providers,) so it may be inappropriate for larger organizations. Also, organizations that only use the SRA Tool to perform their HIPAA risk assessment may overlook the value and importance of engaging with external HIPAA experts.

To best ensure that your HIPAA security assessment catches all potential vulnerabilities, outsource your SRA to a specialist in HIPAA compliance. While it's possible for small providers to complete risk assessments without outside help, partnering with experts will give you a thorough and dependable risk analysis to effectively identify risks, protect data, and better avoid penalties.

Not to mention, a third-party healthcare IT firm is more likely to provide an objective report that identifies overlooked problems and deficient processes. A proper HIPAA security risk assessment includes a consultation so you can get your questions answered, learn simple solutions, discuss the next steps for improvement, and receive training.

Download this HIPAA security risk assessment template checklist to see what you should expect from an assessment. Getting the assessment is only the first step, however. It's what you do with the results that really matters.

5 Critical Steps to Take Once You Receive HIPAA Assessment Results

A comprehensive HIPAA assessment will almost always find problem areas and vulnerabilities that might affect HIPAA security compliance. If you work with an experienced healthcare IT service provider, you should receive a detailed results report following the assessment. This report will flag risks and identify policies, processes, or workflows that should or must be revised.

The good news is that once you know what to address, you can either immediately get to work on fixing the problems or set up processes to monitor shortcomings until you can resolve them. This will help keep your healthcare organization HIPAA compliant and better protect your patients' data.

Here are the five key steps you should take after receiving your HIPAA assessment results.

1. Consult with your HIPAA assessment provider

As stated, a HIPAA compliance risk assessor typically offers a consultation after it delivers your report. You'll be able to ask questions, clarify the issues flagged, discuss the risks involved, learn cost-effective solutions, and discuss how to mitigate the risks.

2. Put your remediation plan into action and document your progress

If you do not act on the recommendations included in your report, you could be putting your patients' PHI and your organization's financial data at risk. In fact, failure to take adequate steps to prevent data breaches could be considered willful neglect under HIPAA regulations. It may result in a civil penalty or worse. For instance, the Texas Health and Human Services Commission was fined $1.6 million for its failure to protect patient data and adequately respond to a potential cybersecurity vulnerability.

Besides taking action to reduce risks and vulnerabilities, document every step you take when implementing your action plan, including progress reports and milestones. HIPAA security compliance requires that you conduct regular assessments, document potential risks, and demonstrate your response. You will need to provide this documentation if your organization undergoes a HIPAA audit.

3. Plan and schedule staff training and education

After undergoing your HIPAA assessment, you will have a clearer idea of your organization's weak spots. As with most security failings, the most likely cause of a data breach is human error. Schedule regular staff training to review what you have

learned from the assessment, including best practices and requirements, so mistakes are avoid or those made in the past are not repeated. Your HIPAA security compliance consultant can advise you on a suitable training and education plan.

Every staff member who works with confidential patient information should receive ongoing education and refresher courses on HIPAA security compliance. This can include everyone from doctors and nurses to IT team, administrative staff, and front desk personnel. The appropriate training will depend on the technology you use, the types of information you process, and the specific needs of your organization. It should cover the following at a minimum:

- ✔ What information is protected under HIPAA regulations, and why it is protected
- ✔ Correct ways of handling protected information
- ✔ Instructions on the compliant use of IT systems, computers, and other data storage systems, especially new systems or workflows

HIPAA training is mandatory for compliance and must be repeated "periodically," according to federal guidelines. You must follow up on your HIPAA assessment with staff training and document all education events and staff attendance.

4. Perform due diligence on business associates

Make sure that your organization as well as all business associates have plans, policies, and procedures in place to help maintain HIPAA compliance. All your business associates must sign and comply with a business associate agreement. They should complete and document their HIPAA assessments and address potential risks. Finally, they should know the correct procedure for notifying you of a cybersecurity incident that affected or potentially affected your PHI and the steps they should take in the event of a breach.

5. Monitor and document your progress, then repeat the assessment as often as necessary

We've said it before, and we'll say it again for emphasis: HIPAA compliance is not a one-time task. It should be an ongoing and continuous effort to handle your patients' confidential information with the utmost diligence and safety. Your healthcare organization must carefully document and implement a plan of action to address risks and vulnerabilities flagged in your HIPAA assessment. You should

also build systems that will allow you to monitor your progress toward resolving or reducing any identified risks.

Plan to repeat your SRA every time you introduce a new IT system, change your data management process, or experience significant turnover or a change of ownership. Also, conduct a regular HIPAA assessment annually to better stay compliant with HIPAA security guidelines.

Give HIPAA Compliance the Attention It Needs

The importance of HIPAA compliance in today's healthcare setting cannot be overstated. On a high level, we know that HIPAA helps healthcare providers maintain a safe, secure, and efficient organization. Yet, the hundreds of pages of HIPAA and related laws can be overwhelming. That's why partnering with healthcare IT with HIPAA-specific expertise is often the most cost-effective way to manage all the moving parts and stay compliant.

Security Risk Assessment: Foundation of Maintaining HIPAA Compliance

Your IT provider should start by conducting a security risk assessment. Not only does it help identify vulnerabilities so you can prioritize your resources, but it also allows you to demonstrate and document your effort in staying HIPAA compliant.

A proper HIPAA SRA can help protect your organization against data breaches, safeguard PHI, and avoid non-compliance penalties. Your healthcare IT partner should then follow up with staff training and regular reporting to help ensure that you remain compliant.

Navigating HIPAA compliance can be challenging for healthcare providers of all sizes. Medicus IT is here to help. We understand HIPAA and the high stakes that come with achieving and maintaining compliance, and organizations nationwide count on us to be their HIPAA backbone. Contact us to see how we help healthcare providers just like yours develop effective HIPAA programs that effectively identify and address vulnerabilities so you can become and always remain HIPAA compliant.

Is it Time to Focus on Your Practice's Technology Wellness?

Learn how Medicus IT's customized solutions and smart, preventive strategies are helping organizations just like yours make the most of their technology.

GET MY FREE CONSULTATION

MEDICUS IT
We do 'IT' Right!

Preventive. Strategic. Deeply Experienced.

www.MedicusIT.com | 844-463-3448