Some Cost Considerations of HIPAA Compliance

As with any regulation, there's a cost-risk element that comes with HIPAA compliance. Developing a culture of compliance and properly protecting PHI costs time and money. Here are several cost factors to consider:

Employee time: Hiring new employees or asking current employees to work overtime to meet HIPAA's standards can easily cost $20 to $30 or more per hour and eat up valuable staff time.

HIPAA training: Depending on the size of your practice, in-house HIPAA training can run from $3,000 to $5,000 per year — sometimes more.

Materials and policies: Medical and dental compliance books can cost up to $500 per year, while legal preparation for Business Associate Agreements and new policies can cost $300 per hour.

Data backup and encryption: Depending on the amount of data your practice is responsible for, backup and encryption solutions can run between $500 and $1,500 — or more.

Asset protection: Asset protection or a cyber insurance policy can cost between $3,000 and $5,000 per year. While coverage isn't required, some level of protection may become instrumental if your practice experiences a cyberattack or other data-related event.

10 Steps to Practical HIPAA Compliance

Practical compliance balances the costs of compliance with the risks of noncompliance. It all boils down to one question:

What amount of resources should you allocate to adequately protect a practice of your size?

Although HIPAA doesn't define how to become compliant and the complexity of the rules can seem daunting, you can easily implement practical compliance by focusing on 10 steps that address the most common vulnerabilities facing many practices:

1 Take a Mandatory HIPAA Risk Assessment

Under § 164.308(a)(1)(ii)(A), conducting a risk assessment is the first step in identifying and implementing safeguards that comply with the standards and implementation specifications in the HIPAA Security Rule.

The assessment is foundational to HIPAA compliance. Therefore, it must be thoroughly understood to address safeguards and technologies that will best protect your PHI. At PCIHIPAA, we've created an online risk assessment tool designed to help practices gain a quick understanding of their key vulnerabilities.

Take our online risk assessment, which will give you a clearer picture of how you can improve compliance. You will immediately receive a risk score to help you evaluate your current state of compliance.

2 Designate a HIPAA Privacy and Security Officer

Next, determine who will be responsible for making sure the rest of your staff is trained and up-to-date on HIPAA policies and procedures. Whether you delegate this responsibility to a single individual or split the work between two, be sure to clearly designate and document the owner(s). HIPAA requires this. Without designating a clear owner, developing a culture of compliance will stagnate.

3 Document All Access to Protected Health Information

It's critical that you understand who has access to PHI and through what devices. Your practice is incredibly vulnerable if you don't fully understand the workflow of your PHI. Alternatively, knowing and monitoring usage will help you identify potential risks and opportunities to shore up weaknesses in your security.

4 Update Policies and Procedures

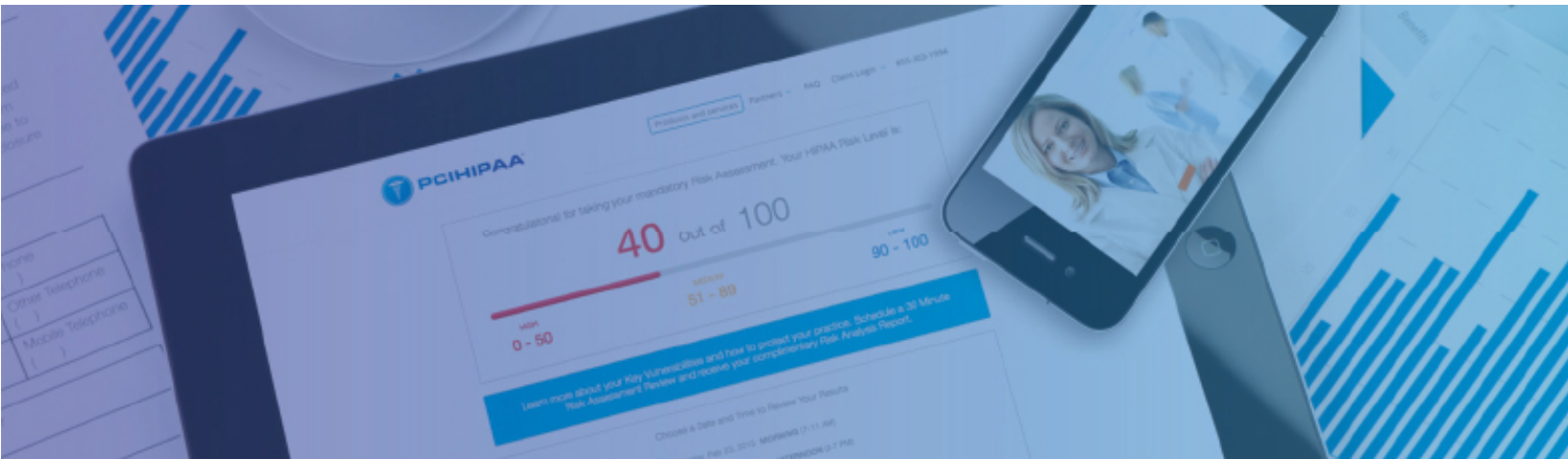
The only way to effectively regulate how your employees protect and handle patient information is to develop appropriate policies and procedures to guide them. Acceptable Use policies, for example, are designed to define what employees can and cannot do regarding PHI, while Sanction Policies define consequences for the improper use of PHI. Your practice is further exposed when you don't have documented policies and procedures to protect your patients' information.

5 Train Your Employees, and Document Their Understanding

There are several ways you can train your employees on HIPAA compliance, and it doesn't have to be overwhelming or interfere with your practice's daily operations. Whether you ask them to watch educational videos, take quizzes, or review your policies and procedures at designated periods, getting started as soon as possible is what matters most. Employees must understand what they can and cannot do when handling protected information, and HIPAA requires documentation to prove their understanding. We created OfficeSafe™ to help practices train employees and properly document their comprehension of compliance.

6 Execute Updated Business Associate Agreements

As a covered entity, your practice is required to execute Business Associate Agreements with anyone (except employees and other covered entities) who handles your PHI to perform his or her work. In September 2013, the Omnibus Rule changed HIPAA requirements regarding these agreements. If you haven't updated your Business Associate Agreements since 2013, you're not in compliance with the law. We've seen covered entities and their business associates fined for not having updated agreements.



7 Create a Disaster Recovery and Incident Response Plan

What would happen if there were a flood, fire, earthquake, or ransomware attack on your practice? Who would you call? How would you contact employees, patients, and key vendors? How would you access PHI and restore your data? These are all questions you must answer and situations you must train your employees on in order to prepare for an emergency. HIPAA requires your practice to be proactive, not reactive. Documenting and testing an Incident Response Plan is an important part of compliance.

8 Make Sure Privacy Documents Are Updated and Utilized

Patient privacy is not the same as data security. Under the HIPAA Privacy Rule, every practice needs a Notice of Privacy Practices that defines how practices can and cannot utilize PHI. Every patient must receive, review, and authorize the notice, and it must be displayed prominently in your practice and on your website. Additionally, patients have to authorize disclosure of their PHI in writing.

9 Utilize Email Encryption and Data Backup Solutions

We see too many practices that still use Yahoo, Gmail, and other free email accounts to handle their electronic communication. These accounts are free for a reason — which was highlighted by Yahoo's recent announcement of a massive data breach and the inadequate security measures that allowed it to happen. If you send any patient information via e-mail, the message must be encrypted so the data remains protected. Don't use thumb drives or other non-encrypted solutions, either. If they're lost or stolen, you'll have been party to a data breach and will have to follow the rigorous notification requirements under HIPAA's Notification Rule. A free e-mail service isn't worth the risk of not having adequate encryption.

10 Obtain Data Breach Coverage

You can obtain specific coverage to cushion the blow of a data breach and resulting HIPAA fines. With the acceleration of data-related incidents and the mass proliferation of data in general, data breach coverage should be an integral part of your risk mitigation strategy.

These 10 steps don't cover all of HIPAA's requirements. However, in today's environment, you have to start somewhere. These steps will help you quickly and affordably mitigate risk and begin to develop a culture of compliance throughout your practice. Your patients' information is one of your most valuable assets, and you need to take steps to protect it. Luckily, you don't have to go it alone.