HIPAA SECURITY CHECKLIST

Things to know BEFORE you start a compliance initiative

Complying with the HIPAA Security Rule is a complex undertaking—because the rule itself has multiple elements that every healthcare business needs to address.

So use this checklist to break the process into logical steps, track your progress and streamline your compliance effort. This road map will help you understand the intent of HIPAA priorities*—**BEFORE** you start building custom compliance strategies.

1. Read "Security 101" (link below)

There are approximately 50 "implementation specifications" in the HIPAA Security Rule, divided into administrative, physical and technical safeguards. So step back! Don't dive into the specifics; spend time understanding the big picture before you drill down into the details. Start with *Security 101 for Covered Entities*, the first of a seven-part series.

2. Determine whether you're a "Covered Entity"

HIPAA applies specifically to "Covered Entities," which include health plans, healthcare providers and healthcare clearinghouses. The full liability of HIPAA compliance also applies to "Business Associates" that work with those "Covered Entities." If your business accesses or handles personal patient data (electronic protected health information, or ePHI) in any way, the HIPAA Security Rule almost certainly applies to you. For more information, see *For Covered Entities and Business Associates*.

3. Identify the right individuals to lead your effort

Appointing an individual to serve as your designated Security Officer is a HIPAA requirement for Covered Entities and Business Associates. Not specifically required, but just as important, is finding a person or people to handle compliance documentation. Seek out team members who have both organizational and writing skills — in that order of priority. A large part of the HIPAA process is not just taking action but documenting what you have done and what you will do. Write down names and specific duties.

4. Make sure you've implemented these basic security measures

Don't get so caught up in the myriad details of HIPAA compliance that you overlook fundamental security. The following is not strictly a HIPAA reference, but it is useful as far as maintaining basic healthcare security: *10 Best Practices for the Small Healthcare Environment*.
Here are some security measures that fall under HIPAA requirements:

- Installing a firewall. While HIPAA doesn't specifically mention the word "firewall," a physical firewall is the only way to adequately protect patient and customer information.
- Installing anti-malware protection and endpoint protection to cover requirements for preventing, detecting and reporting malicious software.
- Using secure authentication, as HIPAA requires strong passwords and/or multifactor authentication to verify that a person or entity seeking to access ePHI is the one claimed.

5. Map your data flows

Be sure to take an inventory of the patient data you control. Document where and how it's stored, how it flows through your organization, and determine where and how individuals have access to it. By understanding vulnerable areas, you'll be better able to address both the *Physical Safeguards* and the *Technical Safeguards*. If you're involved in a relationship between a Business Associate and a Covered Entity, then the HIPAA provisions extend outside your walls and you have special requirements to include provisions for HIPAA security in a contractual relationship. For a sample, see *Business Associate Contracts*.

6. Be able to describe the difference between required and addressable specifications

Most of the required specifications mandate policies and procedures. Addressable specifications involve performing a "risk assessment" and then taking steps to mitigate the risks in a way that's appropriate for your organization. One of the largest HIPAA penalties against a small organization was levied not because an event occurred, but because the organization failed to address the possibility.[1] The *IHS HIPAA Security Checklist* summarizes the specifications and indicates which are required and which are addressable. For an approach to the addressable specifications, see *Basics of Security Risk Analysis and Risk Management*. Another good reference is *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*.

7. Take these steps for a systematic approach

For the addressable specifications and risk assessment, take the following steps:

- Identify the potential threats that you can reasonably anticipate
- Review and document the security measures in place to prevent them
- Evaluate the likelihood that threats will occur and the potential impact and overall risk to the organization
- Prioritize and take action based on your organization's relative risks and resources
- Document your findings, decisions and actions
- Make policies and procedures clear and accessible
- Set up a scheduled, consistent structure for educating and testing staff

Two recommended resources: For larger organizations, refer to *Guide for Conducting Risk Assessments*. For smaller organizations, refer to *Security Standards: Implementation for the Small Provider*.

8. Implement data encryption

Half of all records exposed in reported data breaches involve information on laptops, other electronic portable devices and removable media.[2] If you only do one thing to increase your position relative to a HIPAA Security Rule violation, this is it: Encrypt any protected health information on portable drives, laptops, mobile devices or any other data container that leaves the office — or that might leave the office. Encrypt any data that you transmit via email or other Internet methods. Stolen data that has been encrypted in accordance with HIPAA Omnibus Final Rule has no value to a data thief. Encryption protects your patients' information and provides safe harbor against penalties and patient-notification rules. Here is information on the *Breach Notification Rule* and *Encryption Guidance*.

9. Plan ahead for future reviews

HIPAA requires you to regularly revisit your compliance posture in order to adjust for new vulnerabilities and any changes to your practice or business relationships. The HHS Office for Civil Rights' HIPAA enforcement team conducts random audits of Covered Entities and Business Associates.

This means that even if you haven't been breached, your HIPAA compliance program could come under scrutiny and be subject to fines and civil penalties. The more complete and systematic your documentation, the easier it will be to perform the periodic reviews and you will be less likely to overlook key elements in your compliance profile. For the documentation, retention and update requirements, see *Security Standards: Organizational, Policies and Procedures and Documentation Requirements*.

10. Need help? Hire an expert

Not every organization is able to devote a large share of its administrative or clinical resources to a HIPAA compliance effort, so retaining some outside help often makes business sense. Hiring an experienced network security firm such as ESET, that can assist you with meeting HIPAA compliance related to two-factor authentication, encryption and antimalware protection, can save you time and money.

1—Resolution Agreement, http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

2—Breaches Affecting 500 or More Individuals, http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf

For more information on ESET Industry Solutions for Healthcare, please visit www.eset.com/us/healthcare

** This information is intended to serve as a general resource and guide. It is not to be construed as legal advice. For legal guidance in applying rules created under the HIPAA and HITECH Acts to specific situations, consult an attorney with expertise in this field.*

ENJOY SAFER TECHNOLOGY®