HIPAA SECURITY CHECKLIST

FOR HEALTHCARE

Things to know **before** you start a compliance initiative

25YEARS INNOVATIVE TOP-RATED ANTIVIRUS PROTECTION

Proven. Trusted.

Complying with the HIPAA Security Rule is a complex undertaking because the rule itself has multiple elements. This checklist is not a comprehensive guide to compliance with the rule itself*, but rather a practical approach to help healthcare businesses make meaningful progress toward building a better understanding of HIPAA priorities—before tackling an overall compliance strategy.

1. **See the big picture.** There are approximately 50 "implementation specifications" in the HIPAA Security Rule, divided into administrative, physical and technical safeguards. Don't dive into the specifics; spend time understanding the big picture before you drill down into the details. Start here (it's the first of a seven-part series): Security 101 for Covered Entities.

2. **Understand the applicability of the rule.** HIPAA applies specifically to "Covered Entities," which include health plans, health care providers and health care clearinghouses. It 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 "Security Officer" is a HIPAA requirement. 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. Both a designated security officer and thorough documentation are required parts of the Administrative Safeguards.

4. **Don't overlook the basics.** There are some standard security measures that are prudent and affordable for organizations of any size. These practical and effective safeguards include installing a firewall, installing antimalware protection, and requiring strong passwords and/or multifactor authentication. These proven tools are simple and relatively inexpensive. 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.

5. **Map data flows.** 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. Understand the points of vulnerability and 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. The deadline for compliance was September 23, 2013. For a sample, see Business Associate Contracts.

* This information is intended to serve as a general resource and guide. It is not to be construed as legal advice. For legal guidance as to the application of the HIPAA and HITECH acts to specific situations, consult an attorney with expertise in the field.

HIPAA SECURITY CHECKLIST
FOR HEALTHCARE

Proven. Trusted.

6. **Know with the difference between required and addressable specifications.** Most of the required specifications are about having policies and procedures in place. 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 a systematic approach.** For the addressable specifications and risk assessment, identify the potential threats that you can reasonably anticipate. Review and document the security measures in place to prevent them. Evaluate the likelihood they will happen and the potential impact and overall risk to the organization. Then, prioritize and take action based on your organization's relative risks and resources. Document your findings, decisions and actions. Two recommended resources: Especially 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 (the latter is a bit technical; talk to your network security provider if you need help implementing encryption).

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 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. **If you need help, get an expert**. Not every organization is able to devote a large share of their administrative or clinical resources to a HIPAA compliance effort, so retaining some outside help often makes business sense. There are many reputable consultancies that make HIPAA compliance a major part of their practice, and a network security firm, or managed services provider, that specializes in healthcare technology, might be a right-size resource for smaller organizations.

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

[1] Resolution Agreement, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf

[2] Breaches Affecting 500 or More Individuals, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html