VBM
www.VBMAlaska.com

HIPAA-Compliance Services
Medical Records Scanning
High-Availability Systems
Managed IT Systems
Off-Site Backup / Disaster Avoidance
Point-Of-Care / Tablet Systems

Sword&Shield
ENTERPRISE SECURITY
Security Partner
World-Class Technology, Local Service!

HIPAA / MU Risk Analysis

Overview & Methodology

Overview

A Health Insurance Portability and Accountability Act (HIPAA) gap analysis is the comparison between what exists within an organization and what is required by the HIPAA Security, Privacy, and Breach Notification Rules. The analysis will compare the existing privacy and security policies, procedures and technologies against the privacy and security policies, procedures, and technologies required by the HIPAA rules. There is no measure of risk associated with this analysis; it is merely a comparison of what exists against an interpretation of what the HIPAA regulations require.

The HIPAA Security Rule requires all covered entities and business associates, their agents, and subcontractors to conduct a risk analysis “to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of electronic protected health information.”

Because the security rule applies to a variety of organizations ranging from large healthcare systems to small physician practices, as well as various business associates, the standards are flexible regarding the approach an organization takes based on several factors:

- The organization’s size, complexity, and capabilities
- The organization’s technical infrastructure, hardware, and software security capabilities,
- The costs of security measures, and
- The probability and criticality of potential risks to electronic protected health information (ePHI)

Conducting a Risk Analysis is the first step in identifying and implementing safeguards that comply with the HIPAA Security Rule. A risk analysis is foundational and is a requirement, not an option.

The Risk Assessment will focus on the Polices and Procedures in place at the practice, as well as physical security features (workstation/monitor placement, locked server room, etc.). Depending on the practice’s relationship with the internet, we may recommend an external Penetration Test to test vulnerabilities from internet threats. However, the focus on the Policies and Procedures is key; If the OCR decides to audit your practice, having HIPAA-Complaint Polices and Procedures that address all risk issues identified in the HIPAA rules is key to preventing fines and possibly civil suit liability.

Our Risk Assessment goal is to not only help you be HIPAA-Compliant, but be prepared for an audit, as well.

HIPAA / MU Risk Analysis

Overview & Methodology

Methodology

All ePHI created, received, maintained, or transmitted by an organization is subject to the HIPAA Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of ePHI. Conducting a risk assessment is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule.

The risk assessment is conducted using the guidelines in the NIST SP 800-30, Revision 1, *Guide for Con-ducting Risk Assessments,* published in September 2012. The HIPAA Security Rule does not prescribe a specific risk assessment methodology, but the guidelines set by NIST represent the industry standard for good business practices with respect to standards for securing electronic protected health information (ePHI).1 For ease of use and specific applicability to HIPAA risk assessments, the methodology outlined in the Revision 1 SP has been slightly modified by Sword & Shield subject matter experts.

The first step in a VBM HIPAA Risk Assessment is a kick-off meeting, at which time the IT Service Provider, HIPAA Security and Privacy officer (s) and additional customer points-of-contact are identified. The customer will receive a secure login to the Sword & Shield customer portal for uploading documentation, and we will demonstrate its use at the kick-off meeting.

The Customer will upload all office documents pertaining to HIPAA, such as Policies and Procedures, Employee Handbooks, Notice of Patient Privacy Practices, request for information forms, etc. to the secure portal. VBM prepares an IT questionnaire for the IT Service provider, and may follow-up with some clarification questions.

In the meantime, VBM inspects the physical environment and the IT system as needed depending on the circumstances and relays that information to Sword & Shield. Once the IT interview is complete and all documents are uploaded, Sword & Shield will analyze all of the documentation to determine areas of risk and compliance issues. Sword & Shield will make some broad recommendations on reducing risk in troublesome areas in the Risk Assessment, then VBM will help the customer with a Remediation Plan.

As part of this engagement, VBM will work with the customer to understand the Risk Assessment results, and discuss various options for reducing risk and increasing compliance. VBM will provide recommendations, and help the customer choose the solutions that fit their needs and environment. Once the risk-reduction solutions are chosen, target dates are associated with each solution, and a complete Remediation Plan document is produced that specifies the target solutions and dates to reduce all medium and high-Risk areas to Low-Risk.

In the end, the customer has a plan of action to reduce risk, be HIPAA-Complaint, and be confident that they are ready for an audit.