Elements of a Risk Assessment

The Office of Civil Rights (OCR) has the responsibility to provide guidance to regulated entities about conducting risk assessments. The “Guidance on Risk Analysis Requirements under the HIPAA Security Rule” describes nine (9) essential elements a Risk Analysis must incorporate, regardless of the risk analysis methodology employed. These elements are as follows:

1. **Scope of the Analysis** - all ePHI that an organization creates, receives, maintains, or transmits must be included in the risk analysis. (45 C.F.R. § 164.306(a).)

2. **Data Collection** - The data on ePHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316 (b)(1).)

3. **Identify and Document Potential Threats and Vulnerabilities** - Organizations must identify and document reasonably anticipated threats to ePHI. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

4. **Assess Current Security Measures** - Organizations should assess and document the security measures an entity uses to safeguard ePHI. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

5. **Determine the Likelihood of Threat Occurrence** - The Security Rule requires organizations to take into account the likelihood of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

6. **Determine the Potential Impact of Threat Occurrence** - The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

7. **Determine the Level of Risk** - The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

8. **Finalize Documentation** - The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).)

9. **Periodic Review and Updates to the Risk Assessment** - The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).)

While the OCR does not require the use of the NIST protocols, it does refer to them as the “industry standard for good business practices with respect to standards for securing e-PHI.” No other protocols are mentioned or endorsed by OCR, leaving the burden of proving compliance on the practice. A partial set of the NIST documents needed to do a risk assessment is shown at right.