PUBLICATION

Security Rule Compliance: The Importance of Performing Regular Risk Analyses [Ober|Kaler]

2014: Issue 6 - Focus on HIPAA/Privacy

It is likely that you are familiar with the HIPAA Security Rule's mandate that covered entities and business associates document the decision making process that led to the selection of their means to achieve security for electronic protected health information (ePHI). You probably understand that the security management standard requires covered entities and business associates to implement policies and procedures to prevent, detect, contain, and correct security violations, and that performing a risk analysis is a required implementation specification of that standard. But have you recently gauged your risk analysis to ensure its reliability?

Security risks are constantly evolving and changing over time, particularly because more and more of our protected health information is actually ePHI. Risk assessments should be “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [ePHI] held by the covered entity or business associate.” It is imperative that entities confirm the sufficiency of their risk analyses, as those analyses form the foundation upon which necessary security activities are built.

In the face of the Office for Civil Rights' HIPAA Audit Program, a valid risk analysis is a comforting brace that helps demonstrate to the government that the security precautions implemented by your entity, and the decision not to implement others, are reasonable and appropriate. In determining what is reasonable and appropriate, covered entities and business associates must consider: (i) their size, complexity, and capabilities; (ii) the capabilities of their hardware, technical infrastructure, and software security; (iii) the costs of implementing new security measures; and (iv) the probability and criticality of potential risks to ePHI. Your risk assessment should identify the probability and criticality of potential risks, and should enable your entity to proactively combat those risks.

The regulations do not provide a specific method or “best practice” for performing the risk analysis, and it can be difficult to identify the right or best approach for your particular entity given variations in the size, complexity, and capabilities of covered entities and business associates. The Office for Civil Rights (OCR) has provided guidance on the requirements of conducting a risk analysis to comply with the mandates of the HIPAA Security Rule. The OCR most recently released Guidance on Risk Analysis Requirements under the HIPAA Security Rule (Guidance), which takes into account recommendations from the National Institute of Standards and Technology (NIST). While federal agencies are required to follow the NIST guidelines, covered entities and business associates are not, but they may choose to study the NIST guidelines when performing their compliance duties. NIST offers resources related to conducting adequate risk assessments which are free to the public.

In its Guidance, the OCR provided a helpful framework that your entities should incorporate into their risk analyses, regardless of the method your entity implements. Covered entities and business associates should keep in mind the goal of maintaining confidentiality, availability, and integrity of ePHI as they move through risk assessment. As is evident in the steps below, thorough documentation of your risk analysis is important to your entity's ability to rely on its findings.

1. Identify the scope of the analysis by identifying all of your entity's ePHI.

2. Gather data, including from all locations where ePHI is stored, maintained, or transmitted. This should include a review of past and present projects, conducting interviews and documentation reviews.
3. Identify and document potential threats to ePHI that can be reasonably anticipated (which may be unique to the circumstances of each entity), and vulnerabilities which if exploited could risk inappropriate access to or disclosure of ePHI.
4. Identify, assess, and document current security measures, and determine and document whether your current measures are configured and used properly.
5. Determine the likelihood of threat occurrence/exploitation of vulnerabilities, which your entity should use to inform its determination of what threats can be reasonably anticipated. Document all threat and vulnerabilities with their associated likelihood.
6. Determine the criticality of the impact/magnitude of threat occurrence/vulnerability exploitation on the confidentiality, integrity, and availability of ePHI. Document all potential impacts associated with the threats and vulnerabilities.
7. Determine the level of risk for all identified threats and vulnerabilities and combinations thereof, consider the likelihood and impact values assigned. Document assigned risk levels and mitigating actions to perform.
8. Finalize documentation.

Your entity should consider adding a step 9: Repeat risk assessment periodically. Conducting a risk analysis is not a one-time process; it should be repeated on an ongoing basis. The Security Rule requires entities update and document their security measures "as needed." The best way to determine when security measures need to be updated is by frequently performing risk assessments, particularly when your entity integrates new technologies or business operations. We encourage all covered entities and business associates to review the way in which they conduct their risk analyses to ensure that the processes are well tailored to your entities. A risk assessment is the cornerstone of Security Rule compliance, and we recommend that all covered entities and business associates treat it as such.

145 CFR § 164.308.
245 CFR § 164.308(a)(1)(ii)(A).
368 Fed. Reg. 8346.
445 CFR § 164.306(b).
5*Available at:* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Additional guidance from CMS is available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.
6*Available at:*http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.
7*Guidance on Risk Analysis Requirements under the HIPAA Security Rule* p4-7.
845 CFR § 164.306(e).