Risk Analysis FAQ

The completion of a thorough risk analysis may require collaboration between multiple people, departments, and third-party vendors of your organization—who may be unfamiliar with HIPAA requirements. This guide provides answers to common questions to help you relay the importance of risk analysis requirements throughout your organization.

What is the HIPAA Security Rule?

Many people's understanding of HIPAA compliance is limited to the Privacy Rule, which primarily focuses on how healthcare organizations may use and disclose Protected Health Information (PHI). The HIPAA Security Rule governs who has access to PHI and provides requirements that limit access only to authorized individuals. Compared to the Privacy Rule, the HIPAA Security Rule provides much more detailed and comprehensive requirements to protect PHI.

What is a risk analysis?

A risk analysis is the first step in achieving compliance with the HIPAA Security Rule. The risk analysis is a process designed to ensure healthcare organizations implement policies and procedures that prevent, detect, contain, and correct security violations that put Electronic PHI (ePHI) at risk.

Am I required to complete a risk analysis?

Every organization is required to perform a risk analysis in order to comply with the HIPAA Security Rule. The risk analysis specification requires organizations to:

"conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information". (§ 164.308(a)(1)(ii)(A))

What happens if I don't complete a risk analysis?

Failure to perform a thorough risk analysis can have multiple negative repercussions for your organization, including:

- Increased chance of ePHI loss/theft
- Fines and penalties resulting from violations—up to $50,000 per day
- Loss of patient trust and business
- Severe brand damage

Who is SecurityMetrics?

SecurityMetrics offers risk analysis and other guided assessments to assist healthcare organizations efficiently navigate and comply with the HIPAA standards. SecurityMetrics works with your organization to evaluate your risk environment and provides detailed remediation steps that help you minimize ePHI risk and achieve HIPAA compliance.

In addition to HIPAA assessments, SecurityMetrics is also a provider of PCI DSS, GLBA, and other compliance and data security services. Visit www.securitymetrics.com for more information.