Concluding HIPAA Security Risk Analysis Help

Submitted by: Alan Davis
alan@proteusid.com

Let's finish last newsletter's article discussing the HIPAA Security Rule's Risk Analysis citation. We previously differentiated a risk analysis from a compliance assessment and explained risk analysis frequency strategies. It is our observation that many small or rural healthcare organizations firmly believe that their HIPAA program flies under the Office of Civil Rights radar. But the most recent corrective action plan recipient (as of this writing) is a Colorado critical access hospital, so it's important to get a security risk analysis completed correctly regardless of size or location.

The HIPAA Security program requirement to "…conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability…" of ePHI can result in some head-scratching to provide a reasonable and appropriate risk analysis. But a risk assessment doesn't have to be intimidating or result in an unrealistic workload.

Start a risk assessment with the methodology recognized by the federal government using NIST Special Publication 800-30, Guide for Conducting Risk Assessments. Plan a project that defines your process, risk model and risk measurement. To summarize the NIST material, include:

- a scope that defines the people, places, systems and processes (e.g. policies & procedures)
- all ePHI repositories
- identifying all threats and vulnerabilities
- assessing current security controls
- determining the likelihood and the impact of a risk event happening, and
- using all of these parameters to calculate risk.

A risk may include theft, unauthorized disclosure, fraud, or a number of other events that threaten ePHI security. Risk needs to be quantified (e.g. on a point system) or differentiated (e.g. high, medium, low). The following examples may help improve security and validate a HIPAA Security program, but lack the measures to be considered a bona-fide risk analysis:

- a HIPAA Security Rule compliance evaluation using the 2016 OCR Audit Protocol
- an assessment of information services or technology security controls, even when mapped from a reputable security controls source (e.g. NIST, SANS, etc.) to the Security Rule. This type for work does support the Security Rule's "Evaluation" citation
- completing a checklist. Risk is not "checked".

The output of a risk analysis is a risk register. Once risk is identified, the Security Rule requires that "…Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level…". In simpler terms, *manage that risk*! Identify a person responsible and assign a date to complete the work required. This person needs to determine whether the risk will be:

- avoided (e.g. decommission the risk source)
- transferred (e.g. to another company)
- mitigated (i.e. remedied), or
- accepted.

There are plenty of very thorough information security or auditor-based companies, but we recommend that a Covered Entity or Business Associate organization seek a HIPAA dedicated company to help learn the risk analysis process.