



## Risk Analysis: The First Step Towards HIPAA Compliance

Nicole E. Stratton

*Foster Swift Health Care Law Report*

June 2010

In 2009, the Health Information Technology for Economic and Clinical Health Act ("HITECH") was passed to bolster and expand the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). As part of HITECH's requirements, the Department of Health and Human Services ("HHS") is required to issue annual guidance on HIPAA's Security Rule. HHS recently issued its first guidance on the topic of drafting a "Risk Analysis." In its guidance, HHS touts the Risk Analysis as the "first step" in identifying and complying with the HIPAA Security Rule. The reason for this is the information gathered in completing the Risk Analysis can be used for completing other HIPAA mandated security tasks (such as designing an appropriate personnel screening process).

Overall, the Risk Analysis requires organizations to evaluate "risks" and "vulnerabilities" in order for the organization to take appropriate security measures to protect against reasonably anticipated "threats" to the security of electronic protected health information ("e-PHI"). In order to meet these objectives, the HHS guidance provides definitions to the previously undefined terms of "vulnerability", "threat", and "risk." Moreover, within these definitions, HHS gives examples to illustrate what an organization should be cognizant of when doing its Risk Analysis. For example, the HHS guidance notes that there are common categories of threats (such as natural threats; human threats; and environmental threats) that organizations should take into consideration.

While the guidance notes that there is no specific format required for the Risk Analysis, it does provide a list of the required elements and a brief summary of what is expected for each element. The required elements are: (1) proper scope of analysis; (2) data collection; (3) identify and document potential threats and vulnerabilities; (4) assess current security measures; (5) determine the likelihood of threat occurrence; (6) determine the potential impact of threat occurrence; (7) determine the level of risk; (8) finalize documentation; and (9) periodic review and updates to the Risk Analysis.

---

### **AUTHORS/ CONTRIBUTORS**

Nicole E. Stratton

---

### **PRACTICE AREAS**

E-Health

Health Care

---



---

HHS also noted that while there are uniform required elements, there is no "one-size-fits-all blueprint." For instance, the guidance notes that small organizations will have more control within their environment and, therefore, have fewer issues to consider in determining the sufficiency of their security measures. Moreover, the guidance notes that the frequency of reviewing and updating the Risk Analysis will vary based on the specific organization (some organizations will need to update it annually and others only every three (3) years). Again, the frequency of reviewing and updating the Risk Analysis may depend on a variety of factors such as the size of the organization and whether the organization plans to utilize new technologies or business operations.

The HHS guidance provides a helpful overview, but each organization using e-PHI must perform a unique risk analysis. Contact your legal counsel if you have questions regarding whether your organization utilizes e-PHI and thus must prepare a Risk Analysis.

