March 11, 2014

HIPAA: Back-to-Basics Bulletin Series
Security Risk Analysis

This is the second in a series of bulletins going "Back to Basics" on HIPAA compliance. With the recent changes to HIPAA resulting from the Omnibus Final Rule, this is a good time to reevaluate your organization's compliance with all aspects of HIPAA.

Under the HIPAA Security Rule, covered entities are required to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (ePHI). Once the risk analysis is completed, the entity must take any additional "reasonable and appropriate" steps to reduce identified risks to reasonable and appropriate levels (45 CFR 164.308(a)(1)(ii)).

The HIPAA security risk analysis has become increasingly important to covered entities as it is now required to meet Stage 1 and Stage 2 of meaningful use under the electronic health record (EHR) incentive programs. Although meaningful use does not impose new or expanded requirements on the HIPAA Security Rule, there is one important difference to note. While HIPAA does not mandate how often providers should perform a security risk analysis, meaningful use requires that the analysis must be conducted during *each* reporting period for which the provider attests (i.e., within the 90-day or calendar year period).

There is no single method or "best practice" that guarantees compliance, but most risk analysis processes have commonalities. Below are some steps that should be included in a risk analysis:

- Review the existing security infrastructure in your organization against legal requirements to determine the scope of your analysis.
- Ensure you've gathered all ePHI stored, received, maintained or transmitted by your organization.
- Identify potential threats and vulnerabilities to patient privacy and security.
- Assess current administrative, technical and physical security measures.
- Rate threats and vulnerabilities by likelihood and document your results.
- Document the potential impact of each threat and vulnerability on the confidentiality, availability and integrity of ePHI.
- Use the likelihood and impact to determine the level of risk to the organization for each threat and vulnerability.

After completing these steps and documenting the results, you should create an action plan to eliminate identified security deficiencies and increase efforts to safeguard the confidentiality, integrity and availability of your ePHI.

HIPAA: Back-to-Basics Bulletin Series
Security Risk Analysis

INCompliance offers customized HIPAA consulting services, including audits, training programs and policy and procedure development to help you with the security risk analysis. INCompliance also provides meaningful use attestation audit services. Click here for additional information on our services.

This E-Alert was prepared by Bryn Hunt. Bryn can be reached 614.227.4823 or bhunt@incomplianceconsulting.com. Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com. This E-Alert may be accessed on the INCompliance website.