CapSpecialty℠
A Community of Insurance Specialists

For Small and Medium Practices

HHS Releases New Security Risk Assessment Tool For HIPAA Compliance

Overwhelmed by the requirements for HIPAA compliance? Finding it difficult to decipher the provisions of the HIPAA Security Rule for reviewing administrative, physical and technical safeguards for protecting health information? Worried about the resources needed (including financial) to conduct a proper security risk assessment? You are not alone! The need for guidance, education and tools that help meet the burdens of HIPAA compliance has been expressed by many, especially providers in small and medium size practices.

Conducting security risk assessments (SRA) is an essential requirement for organizations that handle protected health information (PHI). Under the HIPAA Security Rule, these assessments must be performed regularly by providers to find and address vulnerabilities in the safeguards they have in place to protect PHI. Failure to conduct an appropriate SRA has been frequently cited in enforcement actions against providers by the Office of Civil Rights (OCR) of the Department of Health and Human Services (HHS). Large penalties have been imposed on providers who failed to conduct a proper SRA prior to experiencing a data breach.

On March 28, 2014, HHS released a free "Security Risk Assessment (SRA) Guide" designed for small to medium sized practices to assist "in performing and documenting a Security Risk Assessment". The importance of documenting findings from a security analysis, along with a risk management plan to address vulnerabilities in security safeguards, cannot be overstated. The failure to do so is a major finding in OCR investigations and audits of providers. The SRA Tool is a software application that is available for both Windows operating systems and iOS iPads. The press release states "The SRA tool's website contains a User Guide and Tutorial video to help providers begin using the tool. Videos on risk analysis and contingency planning are available at the website to provide further context." (http://www.hhs.gov/news/press/2014pres/03/20140328a.html)

The User Guide makes it clear that the tool is one resource among others that providers can use in implementing the Security Rule and that it does not "produce a statement of compliance" nor include provisions of the HIPAA Privacy Rule. In other words, it is not an overall HIPAA compliance program, but helps with an essential part of an overall compliance program. The website to access the SRA Tool and related information and resources is at:
http://www.healthit.gov/providers-professionals/security-risk-assessment

Although designed for small to medium size organizations, the SRA tool and related resources at the website may be useful as information for all covered entities and business associates about security risk analysis.

HHS has also released the "Top 10 Myths of Security Risk Analysis" which is helpful to educate about and dispel common misconceptions about security risk analyses:
http://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis

Note: Covered entities and business associates, as defined by HIPAA, must comply with the HIPAA Security Rule. Conducting a security risk analysis is a core requirement for payment per the Medicare and Medicaid EHR (electronic health records) incentive plan, i.e., Meaningful Use. Information and definitions about the above, include, but are not limited to:

- Covered entities and business associates
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/
- EHR Meaningful Use Criteria and Privacy and Security of electronic protected health information
  - http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-2.pdf