White Paper: HIPAA Risk Assessment and Compliance Manual

The scope of the Health Insurance Portability and Accountability Act (HIPAA) hasn't changed much since 2003 and 2005 when the Privacy and Security Regulations went into place. While, some changes occurred in 2013 with the Final Omnibus Rule of 2013, one underlying factor that continues to be on the focus for all covered entities and business associates is performing a HIPAA Risk Analysis/Assessment. The HIPAA Risk Assessment creates the foundation and understanding of what the current level of compliance is, as well as understanding areas of risk to the organization. A proper risk analysis/assessment will create a to-do list for each covered entity and business associates that ranks each area of risk from low, medium or high. The benefits of this process is understanding what areas should be addressed quickly and timely as well as the best use of limited time and resources. Based on previous analysis and research, it was clearly documented that the HIPAA Risk Analysis is not consistently completed for covered entities and business associates. The HIPAA Risk Analysis is also a requirement under the EHR Incentive Program, or Meaningful Use, for Eligible Providers and Eligible Hospitals to protect patient information. In the past few years, OCR has assessed fines due to lack of completion of the HIPAA risk analysis:

Fines Assessed to Organizations for Failure to Conduct a Risk Analysis/Assessment:

- **$150,000 – Fine Assessed in response to a data breach –** Anchorage Community Mental Health Services, Inc. for Failure to Conduct a HIPAA Risk Assessment over a 7 year period
- **$400,000 – Fine Assessed in response to a data breach –** Idaho State University for Failure to Conduct a HIPAA Risk Assessment over a 5.5 year period
- **$1,5000,000 – Fine Assessed in response to a data breach** – Columbia University failed to conduct a HIPAA Risk Analysis on all systems that contain PHI
- **$3,000,000 – New York-Presbyterian Hospital -** failed to conduct a HIPAA Risk Analysis on all systems that contain PHI

The HIPAA Compliance manual becomes another necessary tool needed when creating a comprehensive HIPAA compliance program. A detailed HIPAA Compliance Manual will create the policies and procedures within the organization that should be followed for protecting the confidentiality, integrity, and accessibility for protected health information. The following sections regarding policies and procedures are defined out in the HIPAA regulations:

- **HIPAA Privacy Rule – 164.530(i)** - implement policies and procedures regarding PHI that are designed to comply with the Privacy Rule
- **HIPAA Security Rule 164.316(a)** - Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements
- **HIPAA Security Rule 164.316(b)(1)** - Maintain the policies and procedures implemented to comply with the HIPAA Security Rule

Not only is it important to have policies and procedures in place, it is equally important to assure that the policies and procedures are being followed as written. Failure to follow the written policies and procedures that your organizations defines is just as detrimental as not having a HIPAA Compliance Manual with defined policies and procedures in place. In October 2014, an optometry clinic with three ODs had two years of incentive payments (in excess of $40,000) recouped for **failure to have performed a proper risk assessment and failure to follow the policies and procedures** adopted in the HIPAA Compliance Manual.

As we enter 2015, many areas of HIPAA are on the radar for enforcement and evaluation of compliance with the HIPAA regulations. Of the top areas of compliance concerns, the Office of Civil Rights (OCR) lists the HIPAA Risk Analysis/Assessment and Risk Management as the top concern for the HIPAA Security Rule. A complete HIPAA Compliance Manual that creates solid HIPAA policies and procedures is also a top concern of the OCR for the year of 2015. These two areas can create a solid foundation for HIPAA Compliance and should never be overlooked!