PROVIDERS WHO ARE HIPAA COMPLIANT ARE *REQUIRED* TO DO A RISK ASSESSMENT

There are two rules within HIPAA Legislation:

- **The Privacy Rule** (effective since 2003) establishes national standards for the protection of certain health information.

- **The Security Rule** (effective since 2006) established a national set of security standards for protecting certain health information that is ***held*** or transferred in ***electronic form*** (e-PHI).

Within the Security Rule, Administrative safeguards outline several **requirements**: risk analysis, risk management, sanction policy, and information system activity review. All of these have detailed descriptions within the rule.

The Security Management Process standard in the Security Rule ***requires*** organizations to "implement policies and procedures to prevent, detect, contain, and correct security violations." Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard.

Section 164.308(a)(1)(ii)(A) states:

> RISK ANALYSIS (**Required**). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

If a practice ever has a HIPAA violation where PHI is compromised, past compliance with the Security Rule becomes very important. [The HITECH Act (2009) and the Omnibus Rule (2013) provide legal guidelines for HIPAA enforcement and penalties for failures to comply with the law.]

HIPAA violations are expensive. The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision. **Violations can also carry criminal charges that can result in jail time.**

Fines will increase with the number of patients and the amount of neglect. Starting with a breach where you didn't know and, by exercising reasonable diligence (i.e. ***conducting regular Risk Analyses and implementing Security Management processes***), would not have known that you violated a provision, fines range from $100 to $50,000 per incident and does not involve any jail time.

The other end of the spectrum is known as "**Willful Neglect**," where a breach is due to negligence (i.e. ***no effort to assess and reduce risk, or manage security***) and is not corrected in 30 days. Here, fines range from $10,000 to $50,000 for each record and can result in criminal charges.

SUMMARY: In accordance with the Security Rule within HIPAA legislation, all physician practices that hold ePHI are required to conduct Risk Analyses on a regular basis. Most importantly, the process of identifying and correcting risks can protect against a breach. *Should a HIPAA violation ever occur,* having conducted Risk Analyses reduces the risk of large scale, business-disrupting fines.

[Hyperlinks are active in digital format of this document.]

the solutions team Incorporated