February 13, 2015

Do Companies that Handle Personal Health Information Require a Service Organization Control (SOC) Report?

RISK ADVISORY/INTERNAL AUDIT, SOC
BY FRANK DEZORT

The superficial answer is no. Companies that store, process or collect protected health information (PHI) electronically or in paper form are not required to obtain a SOC report by the Health Information Portability and Accountability Act (HIPAA) regulations. However, we are seeing more of our clients that handle PHI or ePHI (electronic protected health information) obtaining SOC 2 reports to demonstrate to their clients that they are complying with Privacy, Security and Breach Notification rules. The SOC 2 report becomes a strong and independent mechanism to objectively communicate the results of the audit assessment against the HIPAA standards.

Use of the SOC 2 report as a vehicle for communicating the results of a third-party HIPPA audit of covered entities or business associates is possible, since the SOC guidance allows the use of recognized industry control frameworks to supplement the Trust Services Principles. The SOC 2 report would include the security (common criteria) and generally accepted privacy principles from the Trust Services Principles along with the Office of Civil Rights control framework.

This would result in a SOC 2 report demonstrating the organization's commitment to mitigating the risks to consumer privacy and independent validation of the level of HIPAA compliance, providing transparency and comfort to clients and prospects. A SOC report would also provide a distinct competitive and marketing advantage to the organization, providing an authoritative and respected method to communicate and demonstrate to the marketplace that protection of private information is as valuable as the quality of the service that it provides.

You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.