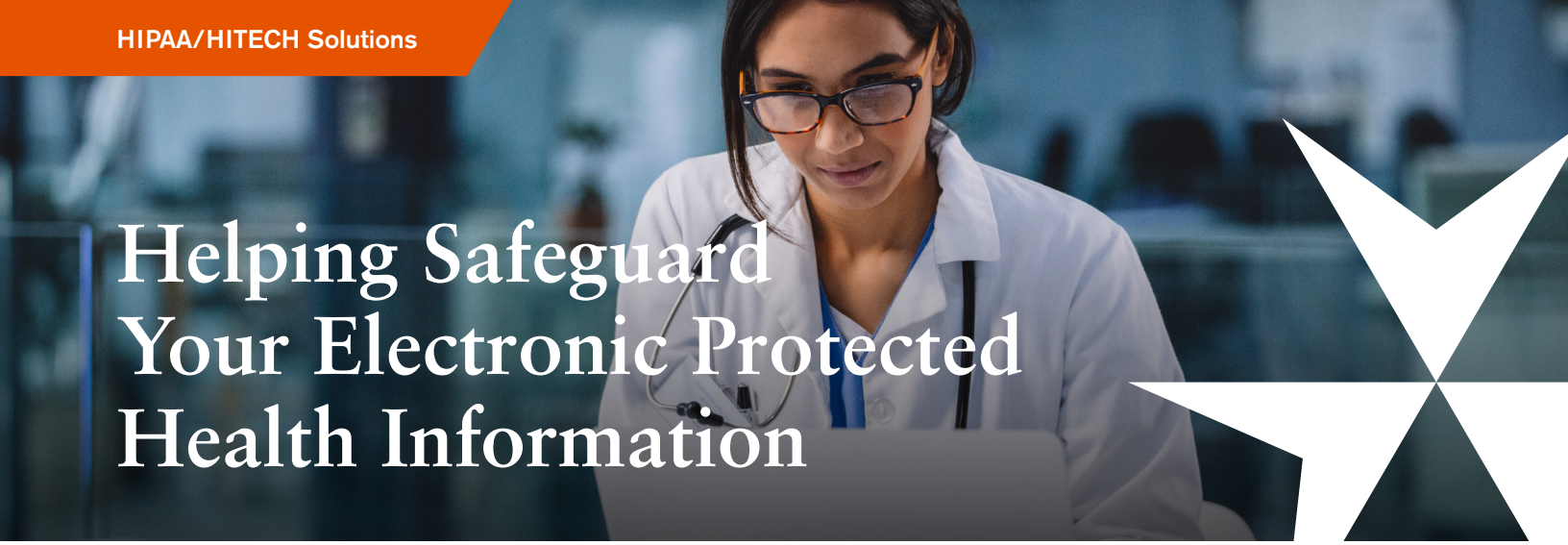

Helping Safeguard Your Electronic Protected Health Information

The HIPAA/HITECH Omnibus Rule of 2013 provides a regulatory framework that is valuable for protecting Electronic Protected Health Information (ePHI).

Fulfilling your obligation as a health plan or business associate to protect ePHI has always been important. However, in today's continuous threat environment, it's crucial to refocus your attention to this critical area. The increased number and sophistication of attacks, combined with stepped up regulatory enforcement activities arising from complaints, breach reports and random audits, means **your data security is under more scrutiny than ever before**.

Failing to comply with the HIPAA/HITECH rules can have severe consequences. Penalties, Resolution Agreements and reputational damage can result in your organization paying millions of dollars per year in civil penalties for a breach of one or more standards, depending on the intent behind the violation.

In addition, the Office of Civil Rights (OCR) may enact a Corrective Action Plan (CAP). CAPs allow the OCR to monitor the progress violators are making to rectify risks and vulnerabilities discovered during an investigation. CAPs may last up to three years and are mandatory, strenuous and continually monitored by the OCR.

Who should perform a HIPAA/HITECH security assessment? Health plans and business associates that:

- Have not conducted a comprehensive security risk assessment as required by the rule in the last three years
- Need more information about industry standards on security and how to evaluate different security alternatives
- Have not implemented data encryption or have implemented it in a limited manner
- Do not destroy data, hardware and media according to HITECH guidelines
- Have not trained their employees to understand they are the first line of defense and provided them with tools to defend accordingly
- Have not updated policies, procedures and other documentation (such as asset inventories)

Segal

We can help

- Conduct a HIPAA Security/HITECH risk assessment.
- Develop and update policies, procedures, disaster recovery plans and business continuity plans.
- Provide staff training.
- Create a process to help monitor your business associates.
- Assist with remediation of risks identified in the HIPAA Security/HITECH risk assessment.

Contact

Jeff Mills
VP, Practice Leader
jsmills@segalco.com
301.908.3014

Michael Stoyanovich
VP, Senior Consultant
mstoyanovich@segalco.com
248.910.2637

Segal is a leading global employee benefits and HR consulting firm delivering trusted advice that improves lives. Visit segalco.com.

Segal