KRIEG DEVAULT

Insights

Have You Conducted A Risk Assessment In A While? If Not, It Could Cost You $400,000

May 17, 2017

By: Stacy Walton Long

On or about December 5, 2011, a hacker accessed email accounts of employees of Metro Community Provider Network ("Metro"), a federally-qualified health center, and acquired 3,200 individuals' electronic protected health information ("ePHI") via a phishing incident[1]. Accordingly, on January 27, 2012, Metro timely submitted a breach report with the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR"). OCR investigated this incident and discovered that, although Metro took the necessary correction action with respect to the phishing incident, Metro did not perform the risk assessment until mid-February 2012. OCR further discovered that Metro's risk analysis was inadequate to satisfy the requirements of the Security Rule under HIPAA, as it failed to address the risks and vulnerabilities identified in a risk assessment.

During the OCR investigation, it was revealed that prior to this phishing incident, Metro had not conducted a risk assessment to determine the risks and vulnerabilities in its ePHI database, and thus failed to implement any related risk management plans to address the risks and vulnerabilities identified in the risk assessment. The Security Rule under HIPAA requires Covered Entities and Business Associates to conduct these risk assessments and implement adequate measures to reduce any identified risks and vulnerabilities.[2] As a result of Metro's failure to conduct this required risk assessment and implement a security management plan to protect ePHI, OCR settled its claims against Metro for $400,000. Since Metro is a federally-qualified health center, and provides various healthcare and social work services to patients who in large part have incomes at or below the poverty level, OCR considered Metro's status when assessing the settlement amount.

[1] "Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels." http://searchsecurity.techtarget.com/definition/phishing.

[2] *See* 45 C.F.R. Sec. 164.308(a)(1).