# HIPAA and Accounting Cybersecurity Update

## 10.16.18

It is a strange combination of events today, but two different agencies released reports on cybersecurity issues that all companies should consider when looking at their systems, controls and checks. The U.S. Department of Health and Human Services ("HHS") was one agency and the other was the Securities Exchange Commission ("SEC").

HHS reported that it had been paid $16.5 Million in penalties, the largest penalty it has received for a HIPAA breach assessment and required substantial corrective action of Anthem, Inc. for its failure to detect and prevent the cyber-attackers access of the protected health information it had on the members of the health plans it insures and that it administers. The corrective action plan requires Anthem to contract for risk assessments on its system with the contract to be reviewed by the HHS and the reports to be provided to HHS. HHS has the ability to revise the statement of work to change what must be done in the risk analysis until it is satisfactory to HHS. Additional policies and procedures are to be adopted and communicated to the work force as well. The risk analysis is to identify vulnerabilities of Anthem's system. Anthem is required to then incorporate the results of the risk analysis into its process for implementing security measures sufficient to reduce risks and vulnerabilities to a "reasonable and appropriate level as required by the Security Rule" and it must provide documentation of such changes to HHS.

**Takeaway:** HIPAA security is not a one and done compliance task. It requires ongoing evaluation of compliance with the HIPAA security standards and it requires periodic risk analysis to be performed on the IT system in which protected health information resides. Periodic review of the HIPAA privacy and security policies for changes in benefits, personnel involved and operating procedures should be done to match operations with the actual policies. HIPAA privacy and security training should be done periodically to keep the workforce aware of the rules and alert to the various types of cyberattacks occurring.

The SEC also issued an announcement today that will be of interest to your accounting colleagues. The SEC had been investigating 9 publicly traded companies who became victims of *"spoofing"* which were emails that purportedly came from executives requesting wire transfers of funds and a *fake vendor scam*. The fake vendor scams were emails from company vendors (following hacking into vendor systems) requesting payment to the vendors but directing the funds to non-vendor accounts. Each of the nine companies with publicly traded securities investigated by the SEC lost at least $1 million, two lost in excess of $30 million and all 9 in total lost nearly $100 million. Because HR requires the use of a number of vendors to deliver benefits, it is important that all of the HR department personnel be alert when reviewing email requests for payment. It is also important that HR department personnel work with the accounting department to devise and maintain a system of internal accounting controls so that fake requests for funds related to HR vendors will not be processed.

The SEC considers that it has jurisdiction to investigate the cyber-attacks because the Securities Exchange Act of 1934 in relevant sections require the issuers of publicly traded securities to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization.

While the SEC decided to not take any enforcement action against the nine companies they investigated, the SEC's report indicated that they were not implying that every company is a victim of a cyber-attack or scam, but it did state, "What is clear, however, is that internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds." It further stated that certain public issuers must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly. For HR departments in those public companies, might expect additional policies and procedures related to cyber threats as those threats continue to evolve.

This SEC report emphasized the importance of all of the company's employees to watch for the cyber threats and to be vigilant. Such vigilance extends to those operating in the HR department. HR departments deal with the employee data in the retirement plan and protected health information in the health plans and other confidential information. HR

departments have dealt with security of the personal information in and related to such plans for some time, this is just a reminder that as threats evolve security measures need to also be reconsidered and evolve.

**Takeaway:** Cyber-attacks and security requirements may come from many directions. Regular updates on threats and security procedures are important to protect the data and the company.

**Contacts:**

Greta Cowart
214.745.5275
gcowart@winstead.com
Marsha Clarke (Admitted in MO and IL)
214.745.5877
mclarke@winstead.com
Nancy Furney
214.745.5228
nfurney@winstead.com
Lori Oliphant
214.745.5643
loliphant@winstead.com