eALERT

INCompliance

March 18, 2016

Failure to execute a BAA results in $1.55 million fine for Minnesota hospital system

On March 16, 2016, the U.S. Department of Health and Human Services (HHS) announced that North Memorial Health Care of Minnesota has agreed to a $1.55 million settlement of potential violations of the HIPAA Privacy and Security Rules. This settlement is the largest to be announced in 2016 thus far, and it is one of the first ever to involve a covered entity's failure to execute a business associate agreement (BAA).

HHS opened an investigation of North Memorial following receipt of a breach report in September 2011. The report indicated that an unencrypted, password-protected laptop, which contained the electronic protected health information (ePHI) of over 9,600 individuals, was stolen from a locked vehicle belonging to an employee of a business associate. The business associate was Accretive, which North Memorial engaged to perform certain payment and health care operations activities. The HHS press release referred to Accretive as a "major contractor" of North Memorial.

The HHS investigation revealed that North Memorial failed to execute a BAA with Accretive, as required under the Privacy and Security Rules. HHS noted in its press release that Accretive had access to the ePHI of nearly 290,000 patients in the North Memorial database. HHS also found that North Memorial had not completed a risk analysis to address all of the potential risks and vulnerabilities to the ePHI. Joceyln Samuels, Director of the HHS Office for Civil Rights, stated: "Two major cornerstones of the HIPAA Rules were overlooked by this entity [….] Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure."

This case is notable for several reasons. First, the settlement amount is quite high and is the first based on the failure to have a BAA in place. Second, this settlement is one of several that have been based on a covered entity's failure to conduct a risk assessment. HHS is clearly sending a message on the importance of these "two major cornerstones" of the HIPAA rules.

In order to protect against a similar fate, covered entities should conduct periodic audits of their contractual relationships to ensure that BAAs are in place with all contractors that are business associates. Additionally, covered entities should not only conduct an initial risk analysis, but should also update the analysis periodically. HHS noted that the risk analysis should cover all aspects of an organization's IT infrastructure, including software and mobile devices. With technology changing ever more rapidly, it is imperative that covered entities review and update their risk analysis to remain compliant with the regulations.

The settlement also raises questions as to whether the indemnity clause that covered entities routinely include in their BAAs goes far enough to fully protect the covered entity when a business associate's breach leads to an investigation that uncovers further violations of the Privacy or Security Rules by the covered entity. Often, an indemnity clause only covers the liabilities related directly to the business associate's breach, as opposed to all liability that may ultimately result from a breach and the investigation of the breach. Covered entities may want to review their BAA indemnity language and consider strengthening the language accordingly.

This Alert was prepared by Chris Bennington. If you have questions, please contact Chris at 513.870.6572 or cbennington@incomplianceconsulting.com or any INCompliance consultant. This and previous Alerts may be accessed on the INCompliance webpage.