Bricker&Eckler ATTORNEYS AT LAW
eALERT
INCompliance

HIPAA settlement with University of Washington Medicine highlights need for organization-wide risk analysis

On December 14, 2015, the Department of Health and Human Services (HHS) announced that it had entered into a $750,000 settlement agreement with University of Washington Medicine (UWM). The settlement resolves allegations that UWM violated the HIPAA Security Rule by failing to implement adequate policies and procedures to detect and correct security violations. While such announcements have become relatively common, the facts of this case include some important lessons for all HIPAA covered entities and business associates.

This settlement was the result of a breach that had been self-reported to HHS by UWM in 2013. The breach report indicated that the protected health information of approximately 900,000 UWM patients was accessed after an employee downloaded an email attachment containing malicious malware. The malware compromised the UWM system, allowing an unauthorized individual to access the protected health information. The breach included patient names, dates of service, medical record numbers, and, for some patients, social security numbers and insurance identification numbers.

The HHS Office for Civil Rights (OCR) launched an investigation in response to the breach report. Because UWM is an affiliated covered entity, the OCR investigation included all of its designated health care components, including the University of Washington Medical Center, other clinical operations and various departments within the university itself. Affiliated covered entities are required to implement appropriate policies and procedures to assure HIPAA compliance with respect to each of the entities that are part of the affiliated group.

The OCR investigation found that, while UWM's policies required all of its affiliated entities to have periodic system-level risk assessments and to implement safeguards in compliance with the Security Rule, UWM did not ensure that all of its affiliated entities were properly conducting the risk assessments and responding to potential risks. OCR Director Jocelyn Samuels stated, "All too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical record or that fails to provide appropriate oversight and accountability for all parts of the enterprise." The HHS press release stressed that covered entities must conduct comprehensive, organization-wide risk analyses to ensure that they "sufficiently address the risks and vulnerabilities to patient data."

The lesson of the UWM settlement is not limited to organizations operating as affiliated covered entities. All covered entities and business associates should review their most recent risk analysis to determine whether it was truly comprehensive in scope. Was the analysis limited to the electronic medical record and other key systems, or did it include all of the organization's systems that could potentially put patient data at risk? In the UWM case, the organization's email

system permitted a message containing malware to reach an employee's inbox, and there was apparently no other system in place to prevent the malicious attachment from opening and compromising the system. If UWM had conducted a more thorough risk analysis and implemented additional security on its systems, the breach and the resulting settlement may have been avoided.

If you have questions regarding HIPAA risk analysis, please contact an INCompliance consultant for more information.