

HIPAA Settlement Illustrates the Importance of Compliance Due Diligence

News May 31, 2019

In any Healthcare M&A transaction, performing thorough due diligence is important. Depending on the nature of the business, this due diligence often includes an assessment of the seller's compliance with the Health Insurance Portability and Accountability Act (HIPAA) and its rules and regulations. The Office for Civil Rights in the US Department of Health and Human Services (OCR) recently announced a Three Million Dollar settlement with a diagnostic medical imaging company related to potential violations of the HIPAA Security and Breach Notification Rules. This settlement arose out of an FTP server which allowed access to protected health information visible on the internet. OCR noted in its press release that notifications to individuals affected by the breach were untimely, an accurate and thorough risk analysis was not conducted, and that business associate agreements were not in place with vendors. For those readers less familiar with prior settlements reached for alleged violations of HIPAA, the lack of a risk analysis and appropriate business associate agreements are common themes seen in settlements and therefore should be appropriately considered in conducting transactional due diligence. For additional detail, please review the Resolution Agreement and Corrective Action Plan.

For additional information contact Paul Welk.