

Largest Single-Entity Settlement to Date Due to HIPAA Non-Compliance

August 11, 2016

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), recently entered into a \$5.55 million settlement agreement with Advocate Health Care Network and its subsidiaries (Advocate) to resolve multiple potential violations of HIPAA involving electronic protected health information (EPHI). The settlement results from OCR's investigation of Advocate which began in 2013 after Advocate submitted three breach notification reports to OCR within a three-month timespan. The reported breaches involved (1) the theft from one of Advocate's support centers of four desktop computers containing unsecured EPHI of nearly four million individuals, (2) unauthorized access of unsecured EPHI from the computer network of Advocate's business associate (BA), and (3) the theft of a laptop containing unsecured EPHI from an Advocate workforce member's vehicle. Upon its investigation, OCR determined that Advocate failed to (a) conduct an accurate and thorough risk analysis related to its utilization of EPHI, (b) implement policies and procedures to limit physical access to its electronic information systems, (c) enter into a HIPAA business associate agreement with the BA, thus causing Advocate to impermissibly disclose EPHI to the BA, and (d) reasonably safeguard EPHI that was maintained at its support center and on the workforce member's stolen laptop computer. In addition to payment of the \$5.55 million settlement amount, the settlement agreement requires Advocate to comply with an extensive, multi-year HIPAA corrective action plan. View a copy of HHS's [press release regarding the settlement](#). View a copy of the [resolution agreement and corrective action plan](#).