Holland & Hart

Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Conduct a Thorough HIPAA Risk Analysis or Pay Big Fines

Insight — 10/26/2016

St. Joseph Health recently agreed to pay $2.14 million to settle allegations by the Department of Health and Human Services Office for Civil Rights Office (“OCR”) that its data security was inadequate.

In its investigation of St. Joseph's handling of a 2012 data breach that exposed 31,800 patient medical records, OCR claimed St. Joseph did not change the default settings on a new server, which allowed members of the public to access via search engines the personal health information of 31,800 patients for a full year. By failing to switch off its servers' default setting, St. Joseph potentially violated the HIPAA Security Rule's requirement to conduct a technical and nontechnical evaluation of any operational changes that might affect the security of ePHI.

In addition to paying $2.14 million, St. Joseph Health agreed to implement a corrective action plan that requires it to conduct an enterprise-wide risk analysis, develop and implement a risk management plan, revise its policies and procedures, and train its staff on these policies and procedures. St. Joseph had conducted an enterprise-wide risk analysis in 2010, but the OCR deemed that to be inadequate because the analysis did not include an evaluation of the technical specifications of St. Joseph's servers.

This settlement indicates that OCR enforcement efforts will continue to focus on investigating the systemic root causes of data breaches – including the failure of healthcare entities to perform accurate and thorough risk assessments. This settlement arrives only a few months after OCR entered into settlements with Advocate Healthcare, Oregon Health & Science University, and the University of Mississippi Medical Center for $5.5 million, $2.7 million, and $2.75 million, respectively. In these cases, the OCR also found the medical centers failed to properly conduct enterprise-wide risk analyses that covered all ePHI, among other things.

To comply with the HIPAA Security Rule, healthcare providers should conduct regular enterprise-wide risk analyses to all, not just some, of its ePHI; implement policies and procedures that limit physical access to electronic information systems; and adopt processes that will identify any changes in their environments, operations electronic, or information systems that might affect the security of ePHI. Any analysis should include a technical evaluation of servers that maintain or transmit ePHI. OCR and HHS have created tools to help entities conduct an effective risk analysis, including HHS' Risk Assessment Tool and OCR's Final Guidance on Risk Analysis.

For questions relating to this healthcare and cybersecurity alert, please

contact Kim Stanger, Romaine Marshall, and Matt Sorensen who are based in Holland & Hart's Boise and Salt Lake City offices.
