HHS Settlement Reminds Covered Entities of Obligations and Potential Penalties under HIPAA

July 24, 2015

The U.S. Department of Health and Human Services (?ÃÂ£***HHS***?ÃÂ¥) recently entered into a Resolution Agreement with St. Elizabeth?ÃÃs Medical Center (?ÃÂ£***SEMC***?ÃÂ¥) to settle charges that SEMC violated HIPAA by failing to implement sufficient security measures to safeguard protected health information (?ÃÂ£***PHI***?ÃÂ¥) when using certain Internet-based document sharing applications. In addition, SEMC allegedly failed to timely respond to, and mitigate damages caused by, the breach of unsecured PHI on an employee?ÃÃs personal laptop and thumb drive. As part of the settlement, SEMC agreed to pay HHS nearly $220,000 and to a corrective action plan under which SEMC must, among other things, review and revise its HIPAA policies, procedures, and training; retrain its workforce who have access to PHI; and submit to certain other reporting and record retention requirements. Employers that sponsor group health plans, in consultation with legal counsel, should undertake a review to ensure full compliance with HIPAA?ÃÃs privacy and security requirements. The Resolution Agreement can be found **here**.