HHS Settlement with HIPAA Covered Entity Exacts $2.5 Million Penalty for Non-compliance

May 30, 2017

The U.S. Department of Health and Human Services?ÃÃ Office for Civil Rights (?ÃÂ£***OCR***?ÃÂ¥) recently announced a $2.5 million HIPAA privacy and security settlement with CardioNet, a wireless health services provider and covered entity under HIPAA, based on CardioNet?ÃÃs impermissible disclosure of unsecured electronic protected health information (?ÃÂ£***EPHI***?ÃÂ¥). The disclosure occurred when a laptop computer belonging to a member of CardioNet?ÃÃs workforce, which contained the unsecured EPHI of 1,391 individuals, was stolen from a parked vehicle outside of the workforce member?ÃÃs home. CardioNet reported the breach to OCR and an investigation ensued, pursuant to which OCR determined that (i) CardioNet did not have a sufficient risk analysis and risk management process in place at the time of the theft, (ii) CardioNet had never actually implemented its draft policies and procedures for compliance with HIPAA?ÃÃs security rules, and (iii) CardioNet was unable to produce any final policies or procedures regarding the implementation of safeguards for EPHI, including those for mobile devices. To resolve these issues, CardioNet agreed to pay a $2.5 million penalty and to implement a corrective action plan. This settlement is another example of the large penalties that HIPAA covered entities, including employer-sponsored group health plans, may be forced to pay to settle HIPAA privacy or security breach actions. The federal government has gotten more aggressive with imposing large fines for violations of these rules and thus employers are well advised to be proactive to ensure compliance. **View the OCR Press Release**?Ã¡announcing the settlement with CardioNet.