Business Associates Beware: OCR Reaches Landmark Settlement with Business Associate for HIPAA Violations

08.03.2016

Amidst a flurry of enforcement actions against covered entities, the Department of Health and Human Services (HHS) recently **settled** with a business associate for $650,000, with a two-year Corrective Action Plan, after its Office for Civil Rights (OCR) concluded an investigation begun in April 2014.

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) is a business associate by virtue of the management services it provides for six nursing facilities. Like many health care entities, CHCS suffered a breach of protected health information, including Social Security Numbers, diagnoses, medications, and names of residents and family, when an unencrypted iPhone without password protection was stolen. A total of 412 individuals were affected. Through the OCR investigation, it was discovered that there were several deficiencies in CHCS' HIPAA compliance.

In addition to the $650,000 fine, the **Corrective Action Plan** mandates the following:

- Development of written policies and procedures related to the HIPAA Security Rule (45 C.F.R. Parts 160 and 164, Subparts A and C)
- Performance of a risk analysis and evaluation of risk management measures
- Security training for workforce members (i.e., employees, volunteers, and others under the direct control of CHCS)
- Notification to HHS if any workforce member violates the new policies and procedures
- Provision of copies of its business associate agreements and management agreements

If CHCS does not comply with the above requirements and all other requirements of the Corrective Action Plan, HHS warns that it would take action and impose a civil money penalty or utilize other available remedies.

Although a $650,000 fine seems substantial, OCR noted that it took into account mitigating factors in calculating the fine, stating that “OCR considered that CHCS provides unique and much-needed services in the Philadelphia region to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS.”

Given that business associates are now directly liable for their compliance with the HIPAA Security Rule and certain requirements of the Privacy Rule (45 CFR Parts 160 and 164, Subparts A and E), we likely will continue to see settlements and enforcement actions levied against business associates. Business associates should prioritize HIPAA compliance and take the time to evaluate and implement their HIPAA policies and procedures, business associate agreements, risk management efforts, and all other measures taken to comply with HIPAA.

Related People