An Active Year for OCR: A 2016 Retrospective of HIPAA Settlements

02.13.2017

Already this year, the Office for Civil Rights (OCR) has **announced** two settlements related to HIPAA violations, totaling over $2.5 million, and the imposition of a civil money penalty of $3.2 million. Before we get too far into 2017, however, OCR?s 2016 settlements provide valuable insight into where covered entities and business associates have had trouble complying with HIPAA, and what the potential consequences for substantial noncompliance might be.

OCR **publicized** 12 settlement agreements with health care providers (and a business associate) in 2016, including the highest single settlement to date, at $5.5 million. Almost all of the investigations leading to the published settlements began with notification to OCR of one or more breaches, with only one arising out of a documented complaint.

The settlements announced by OCR highlighted multiple Privacy Rule and Security Rule issues that the agency identified through its investigations, including lack of authorization for uses and disclosures, improper hybridization of an entity, and failure to timely notify individuals affected by a breach. However, the violations cited most frequently were:

- Failure to conduct a risk analysis, or failure of the risk analysis to evaluate ePHI across the entire enterprise
- Failure to enter into a Business Associate Agreement before disclosing PHI to the vendor or contractor
- Failure to have or failure to implement policies and procedures addressing the Security Rule requirements
- Failure to implement risk management procedures and appropriate security measures to protect against impermissible uses and disclosures of ePHI

These settlements affected different types of providers, from major health systems to physician practices to nursing homes. If a covered entity or business associate thinks it is beyond the reach of OCR, either because of the type of business it conducts, the size of the business, or

the type or amount of PHI it handles, these 2016 published OCR settlements should serve as a warning that there are real consequences for not complying with HIPAA.

Related People