Report on Patient Privacy Volume 19, Number 10. October 10, 2019 OCR Offers Recommendations to Manage, Control 'Insider Threats'

By Theresa Defino

Of the five settlements to resolve allegations of HIPAA violations announced so far this year by the HHS Office for Civil Rights (OCR), four involved actions by either an employee of the covered entity (CE) or its business associate (BA). The lone exception involved a 2015 cyberattack suffered by Medical Informatics Engineering, a BA, which signed a $100,000 agreement with OCR in April, triggered by the exposure of the protected health information (PHI) of 3.5 million individuals.

Two of the others involved unsecure servers, while the most recent centered on comments from a dental office in response to Yelp reviews that contained PHI[1] and a failure to provide a patient with her medical records in a timely manner[2] (see stories, p. 1).

Perhaps it is only fitting, then, that OCR has recently warned in its quarterly cybersecurity newsletter of the need to adopt best security practices with the goal of managing "malicious insider threats."[3]

"Detecting and preventing data leakage initiated by malicious authorized users is a significant challenge facing security professionals today. Identifying potential malicious activity as soon as possible is key to preventing or mitigating the impact of such activity," OCR says in its summer issue (the agency formerly issued security newsletters monthly, but this year it went to a quarterly cycle). "To identify potential suspicious activity, organizations should consider an insider's interactions with information systems."