2017 HIPAA Enforcement: New Settlements and Penalties Already Total Over $11,000,000

03.30.2017

In our last post, we highlighted the 2016 settlements between the Office for Civil Rights (OCR) and various covered entities (and business associates), in one of OCR's most active years. As of now, 2017 is proving to be on pace with last year, with OCR already announcing **three settlements and one civil monetary penalty imposed**, totaling over $11 million.

- On January 9, OCR announced a $475,000 settlement with Presence Health ("Presence"), a health care network located in Illinois, for lack of timely breach notification. Presence experienced a breach of over 800 individuals, and failed to notify the affected patients, the media and OCR within 60 days after discovery of the breach.

- Another settlement was announced on January 18 with MAPFRE Life Insurance Company of Puerto Rico ("MAPFRE"), as a result of a theft of a USB drive that affected over 2,200 individuals. OCR found a lack of risk analyses or risk management plans, despite statements by MAPFRE to the contrary, as well as a continued lack of encryption or similar technology on USB drives and other devices. Settling for $2.2 million, OCR stated in its press release that the settlement amount was attributed in part to MAPFRE's current financial condition.

- On February 1, OCR announced a $3.2 million civil monetary penalty levied against Children's Medical Center of Dallas (CMCD), for violations across multiple years and two breaches. OCR found that CMCD had "actual knowledge" that its security measures were deficient because third-party reports that preceded the breaches identified the security deficiencies at issue. OCR further pointed to a lack of risk management and implementation of encryption or similar safeguards. According to OCR, CMCD was also lacking in its policies and procedures and documentation.

- OCR announced a $5.5 million settlement on February 16, matching the highest settlement to date, with South Broward Hospital District d/b/a Memorial Healthcare System ("Memorial Health"). OCR found that employees of affiliated physician groups had unpermitted access to protected health information, affecting over 100,000 individuals and resulting in fraudulent activity and the sale of PHI. Lacking in sufficient audit controls, Memorial Health also lacked proper policies and procedures governing several significant Security Rule requirements, including audit logs, security incident tracking and workstation access.

As of the date of this blog post, OCR has posted 75 **reports of significant breaches** in 2017, which are attributed to a range of causes, including loss, theft, hacking or other unauthorized access and disclosure. Covered entities and business associates can learn a great deal from these settlements, including areas of focus for OCR and areas of weakness for covered entities and business associates in implementing data safeguards, and should continue to watch OCR's enforcement efforts throughout the year.

Related People