Report on Medicare Compliance Volume 27, Number 37. October 22, 2018
News Briefs: October 22, 2018

By Nina Youngstrom

◆ Anthem Inc., an independent licensee of the Blue Cross and Blue Shield Association, has agreed to pay $16 million to settle potential HIPAA violations in the wake of cyberattacks that resulted in the biggest health care data breach in U.S. history, the HHS Office for Civil Rights (OCR) said Oct. 15. That's also the largest HIPAA settlement ever with OCR. The breach exposed the electronic protected health information (ePHI) of almost 79 million people. Anthem informed OCR in March 2015 that cyber criminals had accessed its IT system undetected through a "continuous and targeted cyberattack for the apparent purpose of extracting data," OCR explained. "Anthem discovered cyber-attackers had infiltrated their system through spear phishing emails sent to an Anthem subsidiary after at least one employee responded to the malicious email and opened the door to further attacks." After investigating, OCR said it concluded that hackers stole names, Social Security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information between Dec. 2, 2014, and Jan. 27, 2015. "Unfortunately, Anthem failed to implement appropriate measures for detecting hackers who had gained access to their system to harvest passwords and steal people's private information," OCR Director Roger Severino said in a press release. Password security and phishing are considered two of the top security risks facing hospitals (RMC 10/8/18, p. 3). Anthem must implement a corrective action plan, conduct a security risk analysis, and review and revise security policies and procedures. It did not admit liability in the settlement. Visit http://bit.ly/2P6Vz8m.