COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 1. January 07, 2021 Privacy Briefs: January 2021

By Jane Anderson

◆ **The HHS Office for Civil Rights (OCR) settled its 13th enforcement action in its Right of Access Initiative**, first announced in 2019 to support individuals' rights to timely access their health records at a reasonable cost under the privacy rule.[1] As part of the settlement, announced Dec. 22, Peter Wrobel, doing business as Georgia-based Elite Primary Care, agreed to take corrective actions and pay $36,000 to settle a potential violation of the right of access standard. In April 2019, OCR received a complaint alleging that Elite failed to respond to a patient's request for access to his medical records, and OCR provided technical assistance in May 2019. However, OCR received a second complaint in October 2019 alleging that Elite still had not provided the patient with access to his medical records and initiated an investigation. In addition to the monetary settlement, Elite is required to follow a corrective action plan (CAP) for two years. The CAP includes implementation of policies and procedures governing the right of access, plus additional training and monitoring.

◆ **GenRx Pharmacy in Scottsdale, Arizona, is warning hundreds of thousands of customers of a data security incident stemming from ransomware.**[2] On Sept. 28, the pharmacy found evidence of ransomware in its system and immediately began an investigation. During the ransomware attack, the pharmacy had full access to its data and unaffected backups, it said. Together with forensic experts, the pharmacy terminated the cybercriminals' access to the pharmacy's systems the same day they were discovered and confirmed that the ransomware had been deployed the day before it was discovered. On Nov. 11, the pharmacy confirmed that the cybercriminals were able to remove a small number of files that included certain health information the pharmacy used to process and ship prescribed products to patients, the pharmacy said. Information that was removed included patient identification numbers, transaction identification numbers, first and last names, addresses, phone numbers, dates of birth, genders, allergies, medication lists, health plan information (including member identification numbers) and prescription information. The pharmacy does not collect patient Social Security numbers. In response to the attack, the pharmacy upgraded its firewall, added additional antivirus and web-filtering software, instituted multifactor authentication, increased Wi-Fi network traffic monitoring, provided additional training to employees, updated internal policies and procedures, and installed real-time intrusion detection and response software on all workstations and servers that access the company network. The pharmacy said it also is assessing further options to enhance its protocols and controls, technology and training, including strengthening encryption.