COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 12. December 09, 2021
Privacy Briefs: December 2021

By Jane Anderson

◆ **Huntington Hospital in New York has sent notices to approximately 13,000 patients about an incident that happened in late 2018 and early 2019 involving a night shift employee who improperly accessed electronic medical records.**[1] The employee was immediately suspended and subsequently fired, and a law enforcement investigation resulted in the former employee being charged with a criminal HIPAA violation. “The hospital cooperated with the law enforcement investigation, which included following instructions to delay notifying any patients who were potentially impacted by this incident through November 2021,” Huntington Hospital said in a statement. “There is no evidence that the former employee accessed Social Security numbers, insurance information, credit card numbers or other payment-related information. The patient information accessed by the former employee may have included demographic-type information such as name, date of birth, telephone number, address, internal account number and medical record number; and clinical information such as diagnoses, medications, laboratory results, course of treatment, the names of health care providers, and/or other treatment-related information.” In addition to its “robust compliance program that includes ongoing training of its employees, implementation of security tools to monitor access to medical record applications, and audits of medical record access,” the hospital said it has “taken additional steps to prevent this type of incident from occurring in the future, including bolstering access controls and targeted re-training of staff on the importance of protecting patient confidentiality.” Huntington Hospital is offering all affected patients complimentary identity theft protection services.

◆ **Southern Ohio Medical Center (SOMC) in Portsmouth, Ohio, was forced to reschedule some procedures and divert ambulances to other hospitals after it was hit with a cyberattack.**[2] “This morning, an unauthorized third-party gained access to SOMC’s computer servers in what appears to be a targeted cyber attack,” the hospital said in a statement. “We are working with federal law enforcement and internet security firms to investigate this incident. Patient care and safety remain our top priority as we work to resolve this situation as quickly as possible. While this does not impact our ability to provide care to current inpatients, we are presently diverting ambulances to other hospitals.” The hospital canceled appointments for medical imaging, cancer services, cardiovascular testing, cardiac catheterization, outpatient surgery and outpatient physical and occupational rehabilitation following the Nov. 11 attack.