Report on Patient Privacy Volume 21, Number 6. June 10, 2021 Privacy Briefs: June 2021

By Jane Anderson

◆ **Scripps Health in San Diego experienced what it called "an information technology security incident" from ransomware that was detected May 1, forcing some of its operations offline.** The attack crippled the health care system's networks, and the system still was struggling to bring everything back online in late May. "We suspended user access to our information technology applications related to operations at our health care facilities, including MyScripps and scripps.org," the health care system said on Twitter on May 1.[1] "While our information technology applications are offline, patient care continues to be delivered safely and effectively at our facilities, utilizing established back-up processes, including offline documentation methods. Our outpatient urgent care centers and Scripps HealthExpress locations and Emergency Departments remain open for patient care." In a letter to patients released May 24, Scripps Health CEO Chris Van Gorder confirmed the cyberattack stemmed from ransomware, but he provided few details on recovery work because "in our current situation, openly sharing the details of the work we have been doing puts Scripps at an increased risk of coming under further attack, and of not being able to restore our systems safely and as quickly as possible for you."[2] The letter stated that "other attackers" are using the information being reported in the media "to send scam communications to our organization," and added that "I know that, for some of you, the reasons why we haven't provided more frequent updates may not matter. But it was important for me to share and assure you that our patients', employees', and physicians' safety and security are our constant guides." The hospital system has not said whether the ransomware resulted in a data breach that compromised protected health information.