Report on Patient Privacy Volume 20, Number 10. October 08, 2020 Privacy Briefs: October 2020

By Jane Anderson

◆ **A former hospital information technology employee was sentenced to 30 months in prison for computer intrusion after compromising dozens of hospital computers**, the Department of Justice (DOJ) announced.[1] Richard Liriano, a New York City resident, engaged in a scheme to use malicious software programs, including keyloggers, on dozens of his coworkers' computers at an unidentified New York City-area hospital, secretly obtaining user names and passwords to his victims' accounts, according to the DOJ. "Using his victims' stolen credentials, Liriano repeatedly compromised their password-protected online accounts, and accessed their sensitive personal photographs, videos, and other private documents," the announcement explained. The incidents took place from 2013 to around 2018, according to the DOJ, and caused more than $350,000 in losses, including remediation expenses, at the hospital where Liriano was employed.

◆ **Millions of people at dozens of health care organizations appear to be affected by a ransomware attack and massive data breach** at one of the world's largest providers of education administration, fundraising and financial management software. More than three dozen health care data breaches related to a May ransomware attack on Blackbaud, a cloud software company that marketed services to nonprofits and charities, have been posted to the HHS Office for Civil Rights website. So far, Inova Health System has reported 1.05 million people impacted, Northern Light Health said 657,000 people were affected, and SCL Health said a total of 441,000 people were impacted.[2] Blackbaud, based in Charleston, South Carolina, said that it discovered and successfully stopped a ransomware attack on its website in May. However, "prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment."[3] That data set did not include financial information or Social Security numbers, the company said. "Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly."