Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 4. April 08, 2021
Privacy Briefs: April 2021

By Jane Anderson

◆ **A Texas Medicaid subcontractor has been terminated after a data breach caused by a ransomware attack originating from Russia exposed the personal information of tens of thousands of low-income residents.** A spokesperson for the Texas Health and Human Services Commission also said that the agency did not learn about the extent of the attack, which occurred last April, until it received questions about the incident from *The Dallas Morning News*.[1] According to news reports, the initial communications to the state agency from the contractor, Accenture, described a multistate incident involving health care providers and insurance billing and collections for health plans. That mirrors other notifications that Accenture's collections subcontractor, Houston-based Benefit Recovery Specialists Inc. (BRSI), made to the federal government and the public last summer, the reports said. Notices the company posted on its website and sent to national news media did not mention Texas Medicaid as the main affected entity, according to news reports. Accenture used BRSI to collect payments from other health insurance plans for pharmacy services provided to Medicaid patients. Accenture told *The Dallas Morning News* that BRSI mailed letters to 130,706 Medicaid recipients to alert them of the breach, but BRSI was unable to mail letters to some breach victims because the stolen data couldn't be traced to specific individuals.

◆ **The FBI's Internet Crime Complaint Center (IC3) received a record number of complaints from the public in 2020: 791,790, with reported losses exceeding $4.1 billion.** The agency said in its 2020 annual report that this represents a 69% increase in total complaints from 2019. Business email compromise schemes "continued to be the costliest: 19,369 complaints with an adjusted loss of approximately $1.8 billion. Phishing scams were also prominent: 241,342 complaints, with adjusted losses of over $54 million," IC3 said in its report. Finally, the number of ransomware incidents also continued to rise, with 2,474 incidents reported in 2020, the report said. In response to these incidents, IC3 said it continues to strengthen its relationships with industry and others in the law enforcement community to reduce financial losses. "Through the Recovery Asset Team, IC3 worked with its partners to successfully freeze approximately $380 million of the $462 million in reported losses in 2020, representing a success rate of nearly 82%," the annual report said. "In addition, IC3 has a Recovery and Investigative Development Team which assists financial and law enforcement investigators in dismantling organizations that move and transfer funds obtained illicitly."[2]