COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 8. August 12, 2021
Privacy Briefs: August 2021

By Jane Anderson

◆ **IBM Security reported that the total cost of a data breach increased by nearly 10% year-over-year in 2021, the largest single-year cost increase in the last seven years.**[1] In its annual *Cost of a Data Breach* report, IBM and the Ponemon Institute said that remote working and digital transformation due to the COVID-19 pandemic increased the average total cost of a data breach. There was a $1.07 million cost difference in breaches where remote work was a factor in causing the breach, the report said. The percentage of companies where remote work was a factor in the breach was 17.5%. Additionally, organizations that had more than 50% of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50% or less working remotely. Information technology (IT) changes "such as cloud migration and remote work increased costs, yet organizations that did not implement any digital transformation changes as a result of COVID-19 experienced $750,000 higher costs compared to the global average, a difference of 16.6%," the study said. In total, data breach costs rose from $3.86 million in 2020 to $4.24 million in 2021, the highest average total cost in the history of the IBM report. The health care sector had by far the highest average total cost of a data breach by industry, more than $9.23 million, up from $7.13 million in 2020. "Costs were significantly lower for some of the organizations with a more mature security posture, and higher for organizations that lagged in areas such as security AI [artificial intelligence] and automation, zero trust and cloud security," the report said. Lost business represented the largest share of breach costs, at an average total cost of $1.59 million, and customer personally identifiable information was the costliest record type, at $180 per lost or stolen record. Compromised credentials were responsible for 20% of data breaches, the IBM report found. Business email compromise was responsible for only 4% of breaches, but had the highest average total cost of the 10 initial attack vectors in the study, at $5.01 million. The second costliest was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million) and compromised credentials ($4.37 million). Organizations with a high level of system complexity had an average cost of a breach that was $2.15 million higher than those that had low levels of complexity, the study found. The presence of a high level of compliance failure was associated with breach costs that were $2.3 million higher than breach costs at organizations without this factor present, according to the report.

◆ **Harris County in Texas said that protected health information for some 26,000 jail inmates was disclosed on a public-facing county website.**[2] "On July 9, 2021, we determined that certain protected health information was inadvertently made accessible" on the county's Justice Administration Department (JAD) website between March 15 and May 22, Harris County said in a notice posted on its website. "The information, provided to JAD as part of the County's legally-required reporting obligations, contained individuals' System Person Numbers (a unique identifier assigned by the Harris County jail system) and some limited health information related to care received at the County's Jail Clinic, such as health history, diagnosis and/or prescription information," according to the statement. "The information did **not** include names, Social Security numbers or financial account/payment information. We have no indication that the information was actually viewed or accessed by any unauthorized person, or that it has been misused; however, we wanted to advise our community of the incident and assure them we are taking this matter seriously." Harris County has set up a dedicated call center to answer questions about the incident.

◆ **UF Health Central Florida has begun notifying patients whose information may have been exposed in a May ransomware incident that forced the health system's Leesburg Hospital and The Villages Hospital onto paper records for almost one month.**[3] The hospitals' electronic health records systems and other IT systems went down from the incident in late May until June 25. According to UF Health, it detected "unusual activity" involving its computer systems on May 31, and "we took immediate action to contain the event, including reporting it to law enforcement and launching an investigation with independent experts." UF Health's Gainesville and Jacksonville campuses were not affected. The investigation determined that unauthorized access to UF Health Central Florida's computer network occurred between May 29 and May 31. "During this brief time period, some patient information may have been accessible, such as names, addresses, dates of birth, Social Security numbers, health insurance information, medical record numbers and patient account numbers, as well as limited treatment information used by UF Health for its business operations," the health system said. "UF Health's electronic medical records were not involved or accessed." UF Health Central Florida said it began mailing notifications to affected patients on July 30.

◆ **UC San Diego Health said July 27 that it had fallen prey to a data breach involving "unauthorized access to some employee email accounts."**[4] The health group said it identified and responded to "a security matter" and that "at no time was continuity of care for our patients affected by the event." UC San Diego Health said it terminated access to the affected accounts and enhanced its security controls. Personal information that may have been accessed or acquired included full names, addresses, dates of birth, emails, fax numbers, claims information (including dates and cost of health care services and claims identifiers), laboratory results, medical diagnosis and conditions, medical record numbers and other medical identifiers, prescription information, treatment information, medical information, Social Security numbers, government identification numbers, payment card numbers or financial account numbers and security codes, student ID numbers, and usernames and passwords. "Once the forensic review has concluded, UC San Diego Health will send individual notices to those students, employees, and patients whose personal information was contained in the accounts, where current contact information is available," the health system said, adding that it will offer one year of free credit monitoring and identity theft protection services to individuals whose data was affected.

◆ **Orlando Family Physicians LLC (OFP), a physician practice located in Florida, said it was the victim of a phishing email that resulted in unauthorized access to four employee email accounts.**[5] The practice said it was "not presently aware of any misuse of the personal information about patients or other individuals contained in the affected email accounts." On April 15, an unauthorized person accessed the email account of a practice employee by obtaining the employee's user ID and password through a phishing email. When a cybersecurity forensics firm began its investigation, it identified three additional employee email accounts that had been accessed. In mid-May, the practice determined that there may have been unauthorized access to personal information contained in the four email accounts, which could have included names; demographic information; health information such as diagnoses, providers and prescriptions; health insurance information; medical record numbers; patient account numbers; and passport numbers. "The available forensic evidence clearly indicates that the unauthorized person's purpose was to commit financial fraud against OFP and not to obtain any personal information about the affected individuals," the practice said.

◆ **Sanford Health in Sioux Falls, South Dakota, was targeted by hacking, but the health system does not believe it was breached.**[6] On Aug. 3, Sanford Health IT staff members were alerted that the system's network was experiencing a hacking disruption. Sanford President and CEO Bill Gassen confirmed in a statement to the *Argus Leader* that the organization was working to resolve the attack. "Sanford Health has experienced an attempted cyber security incident, and we are taking aggressive measures to contain the impact," Gassen said. "Providing patients with exceptional care is our top priority, and we are doing everything possible to minimize disruption." Sanford officials did not provide details on the cyberattack or its impact, other than to say they were not aware of any personal or financial information of patients, residents or employees being compromised by the breach. “We have engaged leading IT security experts to assist in the response, and have notified and will be working closely with federal authorities,” Gassen said.

[1] “How much does a data breach cost?” IBM Security, July 2021, https://ibm.co/3AjAVWm.
[2] Harris County, Texas, “Notice of Privacy Incident Involving County Jail Clinic,” July 27, 2021, https://bit.ly/3lFCOse.
[3] UF Health Leesburg Hospital, “Notice to Our Patients of Cybersecurity Event,” accessed August 9, 2021, https://bit.ly/2VCZDlm.
[4] UC San Diego Health, “Substitute Notice of Data Breach,” July 27, 2021, https://bit.ly/3yvA44r.
[5] Business Wire, “Orlando Family Physicians Experiences Email Phishing Incident,” news release, July 20, 2021. https://bwnews.pr/2VG9F5a.
[6] Joe Sneve, “Sanford Health dealing with cyberattack; no signs of patient data being compromised,” *Argus Leader*, August 4, 2021, https://bit.ly/2VwpoUM.