Report on Patient Privacy Volume 23, Number 3. March 09, 2023 Privacy Briefs: March 2023

By Jane Anderson

◆ **Community Health Systems (CHS), based in Franklin, Tennesse, said in a filing with the Securities and Exchange Commission that Fortra LLC, a third-party vendor, had experienced a breach in its GoAnywhere secure file transfer software, resulting in potential exposure of up to a million patient records.** CHS said protected health information and personal information "of certain patients of the Company's affiliates were exposed by Fortra's attacker."[1] The Clop ransomware group has claimed responsibility for multiple attacks on organizations running GoAnywhere. The HHS Health Sector Cybersecurity Coordination Center (HC3), which first issued a warning about the Clop group in January, reiterated its warning on Feb. 22.[2] "Russia-linked ransomware group Clop reportedly took responsibility for a mass attack on more than 130 organizations, including those in the healthcare industry, using a zero-day vulnerability in secure file transfer software GoAnywhere MFT," HC3 said, noting that Clop claimed it stole information over the course of 10 days and also has the ability to encrypt affected health care systems by deploying ransomware payloads. Clop originally had been written to target Windows systems, HC3 said, but now it appears to have developed a Linux variant. The Linux version is flawed and may allow decryption without paying a ransom, HC3 said, but "the prevalent use of Linux in servers and cloud workloads makes it easy to suggest that Clop could employ this new ransomware campaign to target additional industries, including healthcare."

◆ **A DNA testing firm that suffered a data breach in 2021, exposing Social Security numbers, will pay $400,000 in fines and implement better security practices, the *Philadelphia Inquirer* reported.** DNA Diagnostics Center of Fairfield, Ohio, was alerted repeatedly by a contractor conducting data breach monitoring beginning in May 2021; however, the company overlooked the emails for nearly four months, according to the Ohio Attorney General's office. DNA Diagnostics Center acknowledged that a breach had occurred later in 2021, and news reports indicated that the breach affected more than two million people. Pennsylvania Attorney General Michelle Henry said the breach exposed the Social Security numbers of 12,663 Pennsylvanians subject to genetic testing between 2004 and 2012. Ohio Attorney General Dave Yost said the breach affected approximately 33,000 people in that state. The 18-page settlement between the company and Ohio and Pennsylvania said the stolen information was contained in databases acquired by DNA Diagnostics Center in a 2012 acquisition of Orchid Cellmark. However, DNA Diagnostics claimed that databases were "inadvertently transferred" and that the company "was not aware that these legacy databases existed in its systems at the time of the [2021 breach]—more than nine years after the acquisition." Under the settlement, the company will pay fines of $200,000 to each state attorney general and institute new cybersecurity practices that meet industry standards.[3]