COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 9. September 10, 2020 Privacy Briefs: September 2020

By Jane Anderson

◆ **Utah Pathology Services, based in Salt Lake City, has reported a data breach involving approximately 112,000 patients.** According to the medical practice's "Notice of Data Incident," the practice learned June 30 that "an unknown third party attempted to redirect funds from Utah Pathology."[1] The practice said that this suspicious activity "did not involve any patient information, or the completion of any financial transactions." Upon discovery of the attempted fraud, Utah Pathology said that it quickly secured the affected email account and launched an investigation, with assistance from independent information technology security and forensic investigators. "We discovered that the personal information of certain individuals, including names and one or more of the following personal attributes was accessible to the unauthorized party: date of birth, gender, phone number, mailing address, email address, insurance information including id and group numbers, medical and health information including: internal record numbers and clinical and diagnostic information related to pathology services, and, for a small percentage of patients, Social Security number." There's no evidence that the information has been misused, Utah Pathology said. The practice said it is implementing additional safeguards and security measures, and will provide identity monitoring to affected individuals for one year.

◆ **Developer error caused the leak of 150,000 to 200,000 patient health records stored in productivity apps from Microsoft and Google that were found on the site GitHub, according to a report.**[2] Dutch researcher Jelle Ursem discovered nine separate files of what was termed "highly sensitive" protected health information from nine separate health organizations. The apps involved included Microsoft's Office 365 and Google's G Suite. Ursem said he had difficulty reaching the companies whose data had been leaked, and therefore eventually reported the breach to DataBreaches.net, which worked with him to publish a collaborative paper on the findings. According to the paper, the information was exposed because of developers' improper configuration of access controls and hardcoded credentials in the storing of the information. The leaks were commonly caused by developers embedding hard-coded login credentials into code instead of making them a configuration option on the server, using public repositories instead of private repositories, failing to use two-factor or multifactor authentication for email accounts, and/or abandoning repositories instead of deleting them when no longer needed. In addition, the paper said, errors often went undetected for years because organizations failed to audit their developer's security and compliance with security policies, failed to have a monitored account for researchers to report security concerns, and failed to respond to attempts at responsible disclosure for fear that the notification was a social engineering hack.

◆ **HHS has a new acting chief information officer (CIO).**[3] HHS CIO Jose Arrieta resigned on Aug. 28 "after serving the department since 2019 and following more than 15 years in federal service." Perryn Ashmore, who had been serving as principal deputy CIO, will take over as acting chief information officer, the department announced. Arrieta left "a legacy of transformative advances in our department's data work, better business practices that will save taxpayers hundreds of millions of dollars, and stronger protections for our department's networks from cyber attacks," HHS Deputy Secretary Eric Hargan said in a statement.

◆ **Bad actors are targeting health care research as part of a surge in ransomware, according to a new report from security firm Barracuda Networks Inc.**[4] "Cybercriminals are targeting government, health care and education

organizations with ransomware," and ransoms demanded as part of these attacks are more likely to exceed $1 million, reported Edward Gately from *MSSP Insider*, who reviewed the report. An uptick in attacks was expected due to the upcoming presidential election, the Barracuda report said, but cybercriminals also are leveraging the COVID-19 pandemic and remote work to execute attacks. Attacks on education include the theft of personal information and medical records, as well as health care research. "'With the increased focus on extortion of the breached data, they will likely shift to the sectors where personal data and critical operational data live,'" said Fleming Shi, chief technology officer for Barracuda. "'For example, during a pandemic, they go after health care and higher education, where health research is essential. The level of urgency in getting the data back dictates the willingness to pay.'"

◆ **The Cybersecurity and Infrastructure Security Agency (CISA) said it is "tracking an unknown malicious cyber actor who is spoofing the Small Business Administration (SBA) COVID-19 loan relief webpage via phishing emails.** These emails include a malicious link to the spoofed SBA website that the cyber actor is using for malicious re-directs and credential stealing."[5] The phishing email has been sent to various federal civilian executive branch recipients, along with state, local, tribal and territorial government representatives. The phishing email contains the subject line: "SBA Application – Review and Proceed." It also includes a sender, marked as disastercustomerservice@sba[.]gov, and text in the email body urging the recipient to click on a hyperlink that directs to a page apparently owned by a company called "Leanpro Consulting" in Brazil. CISA listed 15 best practices to strengthen the security posture of an organization's systems, and said that system owners and administrators should review any configuration change prior to implementation to avoid unwanted impacts.

◆ **A cyberattack at Dynasplint Systems Inc., a company in Severna Park, Maryland, that manufactures splint systems for range of motion rehabilitation, may have resulted in the breach of personal data for customers.**[6] According to Dynasplint, the company experienced a data security incident on May 16 and immediately launched an investigation. It engaged a digital forensics firm to determine whether personal or protected health information may have been accessed. On June 4, the investigation determined that certain information was accessed without authorization during the incident and may have included customers' names, addresses, dates of birth, Social Security numbers and medical information. Dynasplint Systems reported the attack to the FBI and will provide free identity monitoring and recovery services to affected individuals.

◆ **Behavioral Health Network Inc., a behavioral health services provider based in Springfield, Massachusetts, suffered what appears to be a ransomware attack.** According to the provider's breach notification, "on May 28, 2020, certain BHN systems became infected with a virus that prohibited access to its files." After an investigation, "BHN determined that an unauthorized actor had placed malware within the BHN environment that disrupted the operation of certain BHN systems."[7] The bad actor gained access to BHN systems between May 26 and May 28, and may have had access to certain files within those systems that contained protected information. The investigation "was unable to determine whether any specific file containing sensitive information was actually accessed or acquired," the company said. Information contained in the affected systems included names, dates of birth, Social Security numbers, medical/diagnosis/treatment information, and health insurance claim information. BHN is providing those individuals potentially affected with access to free credit monitoring and identity protection services.

1 Utah Pathology Services, "Notice of Data Incident," accessed September 8, 2020, https://bit.ly/3hPQxrU.
2 Jelle Ursem and DataBreaches.net, *No need to hack when it's leaking: GitHub healthcare leaks: Protected health information on the public web*, August 2020, https://bit.ly/2Dksq5D.
3 HHS, "HHS Deputy Secretary Hargan Statement on Appointment of Acting CIO," news release, August 28,

2020, https://bit.ly/2QKSLwU.
4 Edward Gately, "Barracuda: Ransom Payments Rise Amid Jump in Attacks," *MSSP Insider*, Channel Futures, August 27, 2020, https://bit.ly/2DplIve.
5 Cybersecurity and Infrastructure Security Agency, "Malicious Cyber Actor Spoofing COVID-19 Loan Relief Webpage via Phishing Emails," Alert, last revised August 14, 2020, https://bit.ly/3bf3YPE.
6 PR Newswire, "Dynasplint Systems, Inc. Provides Notification of Data Security Incident," news release, August 6, 2020, https://prn.to/31Pe4Uo.
7 Behavioral Health Network Inc., "Notice of Data Privacy Incident," accessed September 8, 2020, https://bit.ly/3lPjPcC.