COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 4. April 09, 2020 Privacy Briefs: April 2020

By Jane Anderson

◆ **Health care organizations in the United States, Europe and other world regions are seeing a stark uptick in the number of hacking attempts in the midst of the COVID-19 pandemic**, *Bloomberg News* reports.[1] Some incidents may be related to COVID-19 research or patient care. For example, bad actors broke into computers at Hammersmith Medicines Research, a London-based company that carries out clinical trials for new vaccines just as the company was in talks with other firms for potentially testing a COVID-19 vaccine. The hackers encrypted thousands of patient records and promised to publish them online if a ransom wasn't paid, but the company was able to work with police and its own IT staff to mitigate the damage. Europol, the European Union's law enforcement agency, has received reports of intensifying cyberattacks in almost all of its 27 member countries, and experts say several of the attacks appear to be the work of an organized crime syndicate that uses a strain of ransomware known as Maze. In the U.S., multiple health care providers, such as hospitals, medical laboratories, doctor's offices and urgent care centers, have been hit by ransomware during the crisis.

◆ **As hackers dialed up their attacks on health care entities during the COVID-19 crisis, the Department of Health and Human Services (HHS) was breached by hackers**. Few details were revealed, but a spokesperson for HHS subsequently told *The Hill* that the agency "became aware of a significant increase in activity on HHS cyber infrastructure and are fully operational as we actively investigate the matter."[2] HHS Secretary Alex Azar played down the incident further, saying at a White House news conference that there was "no penetration into our networks" and "no degradation of our ability to function or serve our important mission here."

◆ **A report from Palo Alto Networks reveals that 83% of medical imaging devices are running on unsupported operating systems.**[3] This reflects a 56% jump from 2018 due to the Windows 7 operating system reaching its end of life, and leaves hospital organization vulnerable to attacks that can disrupt care or expose sensitive medical information. The report also uncovered several other threats. For example, it found that 98% of all Internet-of-Things (IoT) device traffic at health care organizations is unencrypted, exposing personal and confidential data on the network and allowing attackers the ability to listen to unencrypted network traffic, collect personal or confidential information, and then exploit those data for profit on the dark web. In addition, 51% of threats for health care organizations involve imaging devices, disrupting the quality of care and allowing attackers to exfiltrate patient data stored on IoT devices. Finally, 72% of health care virtual local area networks mix IoT and information technology assets, allowing malware to spread from users' computers to vulnerable IoT devices on the same network. "Threats continue to evolve and target IoT devices using new sophisticated and evasive techniques, such as peer-to-peer command and control communications and worm-like features for self-propagation," the Palo Alto Networks study says. "Coupled with a weak device and network security posture, attackers have ample opportunity to compromise IoT systems." Some 57% of IoT devices are vulnerable to medium- or high-severity attacks, making IoT "the low-hanging fruit for attackers," the report says. In addition, 41% of attacks exploit device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses, the report says. "We found that, while the vulnerability of IoT devices make them easy targets, they are most often used as a stepping stone for lateral movement to attack other systems on the network," the report authors wrote, noting that password-related attacks on IoT devices are prevalent due to weak manufacturer-set passwords and poor password security practices. Finally, "we're also

witnessing a shift away from attackers' primary motivation of running botnets to conduct [distributed denial of service] attacks via IoT devices to malware spreading across the network via worm-like features, enabling attackers to run malicious code to conduct a large variety of new attacks."

◆ **Ozark Orthopaedics PA, based in Fayetteville, Arkansas, has notified 15,240 patients that their protected health information (PHI) may have been included in a data breach.**[4] Late in 2019, Ozark Orthopaedics noticed "unusual activity" in its email system. After securing the email system, the provider group investigated and found the activity stemmed from four employee email accounts. The investigation revealed that "messages and attachments contained within the affected email accounts included some personal and medical information belonging to Ozark patients," according to the practice. Exposed information may have included patient names, diagnosis and treatment information, health insurance identification numbers, Social Security numbers, and financial account information. Ozark Orthopaedics said in a statement that it "has no evidence that any of the information involved in this incident has been misused."

◆ **Stockdale Radiology in Stockdale, California, reports that it was the victim of a ransomware attack that may have resulted in PHI from some 10,700 patients being exposed.**[5] The practice said the attack took place on Jan. 17, and officials immediately contacted the FBI. "A limited number of files were publicly exposed by the intruder," Stockdale Radiology says in a statement. "In addition, on January 29th, based upon our investigation, we determined that some other files were accessible by the unknown intruder but not exposed." The practice said it was not aware of any misuse of the personal information in the files, which included first and last names, addresses, personal health information and some doctor's notes.

◆ **In Merced, California, Golden Valley Health Centers reported a data breach involving 39,700 patients' information.**[6] On March 3, Golden Valley determined that "a limited number of patients' information" may have been contained in an email account that was accessed by an unknown, unauthorized third party. After identifying potentially suspicious activity, the company's IT staff began an investigation, and determined that medical information, possibly including patients' billing and insurance information, patient referral information, and appointment records may have been contained in an impacted email account. There's no indication that any of the information was misused, according to Golden Valley.

◆ **The Otis Bowen Center for Human Services, which provides mental health and addiction recovery services in Warsaw, Indiana, reports that it suffered a data breach affecting 35,804 patients.**[7] "On Jan. 28, 2020, Bowen Center learned that the personal information of some of its patients and employees contained in two email accounts was potentially exposed to an unauthorized user," the center says in a posted statement. "This discovery was made during the course of an ongoing independent digital forensic investigation." Bowen Center "is unaware of any evidence indicating that anyone's information has been misused as a result of this incident," the statement says.

◆ **San Diego-based Tandem Diabetes Care Inc. said it will be notifying customers of an information security incident involving five Tandem employee email accounts. The incident affected some 140,781 patients**, according to data submitted to the Office for Civil Rights. On Jan. 17, Tandem Diabetes learned that an unauthorized user gained access to an employee's email account through a phishing incident. During the subsequent investigation, forensics experts learned that five email accounts may have been accessed by the unauthorized user between Jan. 17 and Jan. 20. The investigation determined that some protected information was contained in these email accounts, including customer contact information, information related to the use of Tandem's products or services, and/or clinical data regarding customer diabetes therapy. In some very limited instances, customer Social Security numbers were included in the information that may have been breached. As a result of the incident, Tandem is implementing additional email security protocols and is strengthening its user

authorization and authentication processes, company president and CEO John Sheridan says in a statement.[8]

◆ **North Carolina-based Randleman Eye Center said it experienced a ransomware security breach affecting more than 19,000 patients in January.**[9] "On Jan. 12, 2020 we became aware that beginning on or around Jan. 10, 2020, malware was introduced by an unknown third party into some of our systems," the practice says in a statement. "This malware encrypted certain files, including on a server that contained patient protected health information." Data affected included first and last names, dates of birth, genders, and digital retinal images. The practice said there's no evidence that any of the data was compromised beyond encryption, "but that possibility cannot be conclusively ruled out."

1 Ryan Gallagher, "Hackers 'Without Conscience' Target Health-Care Providers," *Bloomberg News*, updated April 1, 2020, https://bloom.bg/2Xg3zHA.
2 Maggie Miller, "Health groups vulnerable to cyberattacks as coronavirus crisis ramps up," *The Hill*, March 16, 2020, https://bit.ly/34cFCSX.
3 Palo Alto Networks, *2020 Unit 42 IoT Threat Report*, March 10, 2020, https://bit.ly/2V3zFDX.
4 Kim DelMonico, "Ozark Orthopaedics Data Breach Exposes Over 15,000 Patients," *Orthopedics This Week*, March 30, 2020, https://bit.ly/2UGq3Qh.
5 Stockdale Radiology, "Data Security Incident," news release, accessed April 6, 2020, https://bit.ly/2xRmvSf.
6 Golden Valley Health Centers, "Golden Valley Health Centers Notifies Patients of Data Breach," *PR Newswire*, news release, March 20, 2020, https://prn.to/2x3RLxx.
7 Otis Bowen Center for Human Services, "Otis Bowen Center For Human Services Notifies Patients of Data Security Incident," news release, March 2, 2020, https://bit.ly/2JHWLKJ.
8 Tandem Diabetes Care, "Tandem Diabetes Care Announces Security Incident with Five Employee Email Accounts," news release, March 16, 2020, https://bit.ly/2UERPwt.
9 Doug Rutledge, "Randleman Eye Center Provide Notice of Data Security Incident," *Yahoo! Finance*, news release, updated March 14, 2020, https://yhoo.it/2yygF8T.