COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 11. November 10, 2022
Privacy Briefs: November 2022

By Jane Anderson

◆ **The second largest nonprofit hospital chain in the U.S. has been grappling with an Oct. 3 cybersecurity incident that affected facilities across the country, forcing ambulance diversions, system shutdowns and patient appointment rescheduling.**[1] CommonSpirit Health has acknowledged a cyberattack involving ransomware "that has impacted some of our facilities" and said that "upon discovering the ransomware attack, we took immediate steps to protect our systems, contain the incident, begin an investigation, and ensure continuity of care."[2] CommonSpirit has 140 hospitals and more than 1,000 care sites in 21 states, and facilities in Iowa, Nebraska, Tennessee and Washington were among those enduring disruptions. MercyOne Central Iowa said the ransomware attack impacted its information systems.[3] Hospital-based systems came back online first, MercyOne Central Iowa said. However, as of late October, access had not yet been restored for patient electronic health records and electronic prescription tools, and patients were unable to schedule appointments online, the hospital system said. "It will take some time before we can restore full functionality, and we continue work to bring our systems up as quickly and safely as we can," MercyOne Central Iowa said.

◆ **A former pharmaceutical sales representative from Berkeley, New Jersey and a Delray Beach, Florida physician have pleaded guilty in a scheme that involved defrauding New Jersey state health benefits programs and other insurers out of more than $2.5 million,**

U.S. Attorney Vikas Khanna said.[4] Keith Ritson and Frank Alario, MD, had been charged in 2020 in a 16-count indictment. Ritson pleaded guilty to one count of conspiracy to commit health care fraud and one count of conspiring to wrongfully disclose health information in violation of HIPAA. Alario pleaded guilty to conspiring to wrongfully disclose patients' individually identifiable health information. According to the original indictment,[5] Ritson and Alario recruited individuals to obtain very expensive and medically unnecessary compounded medications from a Louisiana pharmacy, Central Rexall Drugs Inc. Ritson and Alario learned that certain compound medication prescriptions—including pain, scar, antifungal and libido creams, and vitamin combinations—would be reimbursed by insurance providers in amounts in the thousands of dollars for a one-month supply, the indictment said. The two men also learned that some New Jersey state and local government and education employees had insurance coverage for these compounded medications, according to the indictment. "As a sales representative not affiliated with Alario's medical practices, Ritson should not have had access to patients' confidential information. However, since only certain insurances covered the compound medications promoted by Ritson, the defendants accessed patient files and other identifying information to ascertain patients' insurance coverage," the U.S. Attorney's Office said. "On at least one occasion, Ritson and Alario jointly accessed patient information on an office computer for the purpose of determining insurance coverage for the medications. Ritson also had access to parts of Alario's office where patient information was stored or could be heard and observed, including employee-restricted areas with medical files, fax machines, and computers. Ritson was also frequently present in exam rooms during patient appointments with Alario for the purpose of promoting the compound medications."

◆ **Three federal agencies are jointly warning that ransomware promulgated by the Daixin Team, a cybercrime**

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

group that is actively targeting U.S. businesses, is on the rise among health care entities.[6] Since at least June 2022, Daixin Team cybercrime actors have caused ransomware incidents at multiple health care and public health sector organizations, the U.S. Department of Health & Human Services, the Department of Justice and the Cybersecurity & Infrastructure Security Agency said in a joint bulletin. The Daixin team has deployed ransomware to encrypt servers responsible for health care services, including electronic health records services, diagnostics services, imaging services and intranet services, the bulletin said. The cybercrime actors also have exfiltrated personal identifiable information and patient health information, and threatened to release the information if a ransom is not paid, the agencies said. "Daixin actors gain initial access to victims through virtual private network (VPN) servers," the bulletin said. "In one confirmed compromise, the actors likely exploited an unpatched vulnerability in the organization's VPN server. In another confirmed compromise, the actors used previously compromised credentials to access a legacy VPN server that did not have multifactor authentication enabled. The actors are believed to have acquired the VPN credentials through the use of a phishing email with a malicious attachment. After obtaining access to the victim's VPN server, Daixin actors move laterally via Secure Shell and Remote Desktop Protocol." The three agencies advised health care entities to patch systems, require multifactor authentication and train users to recognize phishing attempts.

◆ **The FBI said it has received multiple reports of cybercriminals increasingly targeting health care payment processors to redirect payments.** In each of these reports, the FBI said, unknown cyber criminals used employees' publicly available personal identifiable information and social engineering techniques to impersonate victims and obtain access to files, health care portals, payment information and websites. In one case, the attacker changed victims' direct deposit information to a bank account controlled by the attacker, redirecting $3.1 million from victims' payments. In another example, which occurred in April, a health care company with more than 175 medical providers discovered an unauthorized cybercriminal posing as an employee had changed Automated Clearing House instructions of one of their payment processing vendors to direct payments to the cybercriminal, successfully diverting approximately $840,000. FBI said the cybercriminals are using phishing emails—specifically targeting financial departments of health care payment companies—and that it expects the efforts will continue.[7]

◆ **The Valley Hospital in Ridgewood, New Jersey, said it was notifying patients about a privacy incident after documents were mistakenly discarded.**[8] The hospital, part of the Valley Health System, said it was informed that post-COVID-19 testing patient instructions were thrown away in a marked recycling bin at an outpatient COVID-19 testing facility. Upon learning of the incident, the hospital attempted unsuccessfully to retrieve the improperly discarded documents. Through its investigation, The Valley Hospital said it determined that the instructions included the names of providers administering the COVID-19 test and were labeled with patient names, medical record numbers, service dates and location codes for the scheduled procedure. The instructions did not include patient addresses, phone numbers, insurance identification numbers, Social Security numbers, positive or negative COVID-19 status, procedure type "or any other information that constitutes protected health information," the hospital said. There's no evidence that any of the instructions were accessed or acquired, the hospital said, but "we cannot rule out that possibility. Thus, out of an abundance of caution, The Valley Hospital is notifying all patients tested at that facility between June 1, 2022, and September 1, 2022."

◆ **Michigan Medicine has reported its second breach this year, saying that a phishing scam led to possible disclosure of health information for some 34,000 patients.**[9] Officials said a cyberattacker targeted Michigan Medicine employees with phishing emails, and four employees were lured to a website between Aug. 15 and 23 and entered their Michigan Medicine login information, allowing the attacker to access their email accounts. Health system officials learned of the hacks and disabled the accounts Aug. 23. Some emails and attachments contained identifiable patient information, such as names, medical record numbers, addresses, dates of birth and other health- and insurance-related information, Michigan Medicine said.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

[1] Tim Starks, “An ‘unprecedented’ hospital system hack disrupts health-care services,” *The Washington Post*, October 6, 2022, https://wapo.st/3NI9s8A.
[2] CommonSpirit, “CommonSpirit Update,” news release, October 17, 2022, https://bit.ly/3SP40BV.
[3] MercyOne, “MercyOne Central Iowa continues to provide the highest quality care to patients,” news release, November 1, 2022, https://bit.ly/3U8yy2p.
[4] Jenna Calderón, “Berkeley man pleads guilty to scam to get paid for unneeded prescription drugs,” *Asbury Park Press*, October 20, 2022, https://bit.ly/3ztKfce.
[5] U.S. Department of Justice, U.S. Attorney’s Office, District of New Jersey, “Physician and Sales Representative Charged in $2.5 Million Health Care Fraud and with Unlawful Disclosure of Patient Information,” news release, September 10, 2020, https://bit.ly/3Fv5w96.
[6] U.S. Department of Health & Human Services, Department of Justice, and Cybersecurity & Infrastructure Security Agency Joint Cybersecurity Advisory, “#StopRansomware: Daixin Team,” October 21, 2022, https://bit.ly/3DjPbl7.
[7] Federal Bureau of Investigation, Cyber Division, “Private Industry Notification: Cyber Criminals Targeting Healthcare Payment Processors, Costing Victims Millions in Losses,” September 14, 2022. https://bit.ly/3SII9fM.
[8] Valley Health System, “The Valley Hospital Addresses Patient Privacy Incident,” news release, October 13, 2022, https://bit.ly/3DLKL7Z.
[9] Briana Rice, “Michigan Medicine: Data breach could have exposed health care information of more than 34k patients,” Michigan Radio, October 27, 2022, https://bit.ly/3zwTg4q.

This publication is only available to subscribers. To view all documents, please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website’s Terms of Use.