COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 10. October 06, 2022 Privacy Briefs: October 2022

By Jane Anderson

◆ **Thirty Democratic senators led by Sen. Patty Murray, D-Wash., have called on HHS to strengthen federal privacy protections under HIPAA to broadly restrict providers from sharing patients' reproductive health information without their explicit consent**—particularly with law enforcement or in legal proceedings over accessing abortion care. The push from Murray, who chairs the Senate Committee on Health, Education, Labor and Pensions, and her colleagues comes as legislators and prosecutors have sought to enforce states' abortion bans by investigating women and doctors. "The *Dobbs v. Jackson Women's Health Organization* decision has caused widespread confusion among health care providers on health privacy protections, and whether they are required to turn over health information to state and local law enforcement," the senators wrote. "To safeguard the privacy of women's personal health care decisions and ensure patients feel safe seeking medical care, including reproductive health care, we urge you to quickly initiate the rulemaking process to strengthen privacy protections for reproductive health information."[1]

◆ **A Johns Hopkins anesthesiologist and her spouse, a U.S. Army major and military doctor, conspired to share highly sensitive medical records with Russia, according to a federal indictment filed Sept. 28.** Anna Gabrielian and Maj. Jamie Lee Henry allegedly communicated to someone they believed was working for the Russian government, but who actually was an FBI agent working undercover. The pair allegedly told the FBI agent that they were willing to provide the medical records of military personnel and certain patients of Johns Hopkins Hospital. The indictment only refers to Johns Hopkins as "medical institution," but Gabrielian, 36, lists Johns Hopkins Hospital as her employer on her LinkedIn profile. "We were shocked to learn about this news this morning and intend to fully cooperate with investigators," a spokesperson for Johns Hopkins Medicine told a local media outlet. The indictment said Henry, 39, held a secret level security clearance, which permits an individual to access information classified secret, "the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security." Henry was stationed at Fort Bragg in North Carolina. The two are charged with conspiracy and offenses related to violating HIPAA. Gabrielian allegedly met with the undercover FBI agent at a Baltimore hotel on Aug. 17. The anesthesiologist told the agent she had previously reached out directly to the Russian Embassy by email and phone to offer her and Henry's assistance after the nation invaded Ukraine, the indictment alleges.[2]

◆ **HHS Health Sector Cybersecurity Coordination Center (HC3) is warning health care organizations about Evil Corp, which it termed "one of the most capable cybercriminal syndicates in the world."** The syndicate is based in Russia and has been operational since 2009, HC3 said in a threat profile, and has been responsible for the development and operation of several of the most powerful malware and ransomware variants. Evil Corp maintains "strong relationships not just with other powerful cybercriminal gangs, but also the Russian government," HC3 said. According to the bulletin, ransomware from Evil Corp is the most significant threat to the health care sector, but data theft and intellectual property theft are also threats. "Foreign governments often find it to be more cost effective to steal research and intellectual property via data exfiltration cyberattacks rather than invest time and money into conducting research themselves," HC3 said. "It is entirely plausible that Evil Corp could be tasked with acquiring intellectual property from the U.S. health sector using such means at the behest of the Russian government."[3]

◆ **A Maryland woman accused of stealing credit and debit card information from her employers, a Walgreens and an urgent care clinic, and using the stolen cards to shop online, has been charged with 120 counts of theft and fraud, police said.** Jayonna Best is accused of photographing credit and debit cards of patients obtaining services at Your Doc's Inn in Cambridge, Maryland, and at her prior place of employment, a Walgreens also located in Cambridge. The cards allegedly were used to purchase various items online from November 2021 to Sept. 7, 2022, according to police. "She stole $519 from my debit card," Carla Ramos, a Maryland resident, told *McClatchy News*. Ramos said she visited the urgent care clinic in early September and saw the woman working there. That same day, fraudulent payments began to appear on her account. "I'm sure it was her," Ramos said. "She was shopping on Etsy." Police are urging any additional potential victims to come forward.[4]

◆ **Home health care company Right at Home, based in Omaha, Nebraska, fired one employee and reprimanded another following a HIPAA violation in the Vermillion, S.D., area,** the company told the *Argus Leader*. The company offers companion, personal, nursing care and specialty care for seniors and adults with disabilities. Few details about the case have been released, and the patient involved declined to speak on the record. Attorney Harry Jones, who represents Right at Home, said that "there's been accountability in a very strict way. That's not the same as saying there's been a criminal violation or a civil violation. But way before that, RAH [Right at Home] doesn't want people breaking their actual internal policies, so it wasn't done the right way."[5]

◆ **Ambulance service Empress EMS, based in Westchester County, New York, reported a data breach affecting 318,558 patients after a security incident that likely involved the Hive ransomware gang.** Hive reportedly contacted Empress to inform the company that it had stolen more than 280 gigabytes of data, including business files, private company information, and employee and customer data. The incident, which occurred in July, compromised Social Security numbers, dates of service and the names of insurers, according to Empress EMS. Hive posted about the attack on its leak site in July but removed it soon after. Empress EMS said it will offer a free 12-month membership to Experian IdentityWorks Credit 3B—a service focused on identity theft—to those whose information was compromised. It also said it is implementing new network security measures and providing additional training to its employees to help prevent future attacks.[6]

◆ **Heartland Healthcare Services, a pharmacy company co-owned by HCR-ManorCare and CVS Health, has notified patients that it was the target of a ransomware attack in April, and personal information may have been exposed**. The attack, which Heartland said involved Heartland Pharmacy of Pennsylvania, Heartland Pharmacy of Maryland and Heartland Pharmacy of Illinois, was discovered on April 11. Heartland said it learned of the attack when it received a ransom demand and immediately contacted the FBI. "Heartland consulted with the FBI regarding paying the ransom," the company said in its breach notification. "Ultimately, Heartland did not pay the ransom. We have since learned that the misappropriated files have appeared on the dark web." Protected health information that was exposed included: addresses, phone numbers, medication names, and other medication information, Heartland said.[7]

◆ **A Texas hospital said its systems are recovering following a ransomware attack that occurred on Sept. 1.**The Richmond, Texas-based OakBend Medical Center said its IT teams took all systems offline and put them in lockdown mode, securing all patient-centric systems as soon as the attack was discovered. The attack caused communication issues, and the hospital set up a temporary email address for patients, vendors, medical staff, administrators and employees. As of Sept. 30, the hospital said all of its clinical systems were back online or had replacement operations in place. "We have engaged an electronic forensics company to help us identify the extent of the data theft and those who may have been impacted," the hospital said. "We are also working with a cyber security firm to improve our system defenses, monitor for future threats, and thoroughly investigate the attack."[8]

---

1 Sen. Patty Murray, "Murray Leads 29 Senators in Urging Biden Admin to Strengthen Privacy Protections for Women Seeking Reproductive Health Care," news release, September 13, 2022, https://bit.ly/3fzvf5D.
2 Paul Gessler, "Hopkins anesthesiologist, Army Major spouse conspired to offer medical records to Russia: federal indictment," CBS News Baltimore, September 29, 2022, https://cbsn.ws/3y1N5nV.
3 The Department of Health & Human Services Health Sector Cybersecurity Coordination Center, "HC3 Threat Profile: Evil Corp," August 29, 2022, https://bit.ly/3E7Y5nN.
4 Brenda Rascius, "Health worker photographed patient credit cards and went shopping with them, cops say," *Merced Sun-Star*, September 28, 2022, https://bit.ly/3E3bltX.
5 Trent Abrego, "Right at Home employee fired after HIPAA violation in Vermillion, attorney says," *Sioux Falls Argus Leader*, September 27, 2022, https://bit.ly/3Rscbn4.
6 Jeff Edwards, "300K Patients' Data Compromised In Ransomware Attack On Empress EMS," *Patch*, September 22, 2022, https://bit.ly/3SHv8DP.
7 Heartland Healthcare Services, breach notification letter, September 2022, https://bit.ly/3y8m1DH.
8 OakBend Medical Center, "Important Announcement" and "Updates," September 30, 2022, https://bit.ly/3fv1EKr.