COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 9. September 07, 2022
Privacy Briefs: September 2022

By Jane Anderson

◆ **More than 92% of patients believe privacy is a right and their health data should not be available for purchase, according to a survey from the American Medical Association (AMA).** The survey of 1,000 patients was conducted by Savvy Cooperative, a patient-owned source of health care insights, at the beginning of 2022. It found concern over data privacy protections and confusion regarding who can access personal health information. Nearly 75% of patients expressed concern about protecting the privacy of personal health data, and only 20% of patients indicated they knew the scope of companies and individuals with access to their data. This concern is magnified by the U.S. Supreme Court ruling in *Dobbs v. Jackson Women's Health Organization*, as the lack of privacy data could place patients and physicians in legal peril in states that restrict reproductive health services, the AMA said. The survey indicated patients are most comfortable with physicians and hospitals having access to personal health data and least comfortable with social media sites, employers and technology companies having access to the same data. Some 94% of patients want companies to be held legally accountable for using their health data, and 93% want app developers to be transparent about how their products use and share personal health data. Almost 80% of patients want to be able to opt out of sharing some or all of their health data with companies, and more than 75% of patients want to opt in before a company uses any of their health data.[1]

◆ **A report from cybersecurity firm Cynerio and the Ponemon Institute found that 56% of health care organizations experienced one or more cyberattacks in the past 24 months involving Internet-of-Medical-Things and/or Internet-of-Things (IoMT/IoT) devices.** Some 45% of respondents to the survey reported adverse impacts on patient care from these attacks, and 53% of those (24% of the total surveyed) reported adverse impacts resulting in increased mortality rates. Out of the 43% of respondents who suffered at least one data breach in the 24 months prior to the survey, 65% suffered an average of five or more data breaches and IoT/IoMT devices were involved 88% of the time, the survey said. "Respondents were asked to estimate the total cost of the one largest data breach involving an IoMT/IoT device including direct cash outlays, direct expenditures, indirect labor costs, overhead costs and lost business opportunities. The average total cost of the largest data breach was estimated at $13 million for the organizations represented in this research." Organizations gave a variety of answers when asked which roles were primarily responsible for the security of IoMT/IoT devices, indicating "there is no widely accepted ownership," the study found. And, although perceived risk of these devices is rated high by 71% of respondents, only 21% reported "a mature stage of proactive security actions," the report said.[2]

◆ **An employee at Phoenixville Hospital in Phoenixville, Pennsylvania, was fired after viewing patients' medical records without authorization, according to the hospital's parent company.** Tower Health, which operates the hospital, said the incident was discovered as part of the hospital's routine monitoring of employees' access to patients' electronic medical records. A recent review showed an employee accessed a patient's medical records on May 1 without any apparent legitimate reason. Hospital officials began an investigation that ultimately showed the employee had accessed the medical records of several patients between October 2021 and May 1. The employee was immediately suspended and later fired. Hospital officials did not specify what role the employee filled at the hospital. The information that was improperly accessed included names, addresses, dates of birth and appointments at the hospital, diagnoses, data on vital signs, medications, test results, and notes, according to hospital officials. In some instances, partial Social Security numbers, the names of medical insurance providers and medical insurance identification numbers also were viewed. Phoenixville Hospital has contacted affected patients and will provide free credit monitoring for those whose partial Social Security numbers and medical insurance information was accessed.[3]

◆ **Two U.S. lawmakers asked HHS Secretary Xavier Becerra for a briefing on the status of efforts to protect the health care and public health sector from cyberthreats, with a special emphasis on collaboration with the private sector.** In an Aug. 11 letter to Becerra, Sens. Angus King, I-Maine, and Rep. Mike Gallagher, R-Wis., noted that ransomware attacks on health care and public health targets have skyrocketed since the beginning of the COVID-19 pandemic. King and Gallagher said they "were heartened" that the White House hosted an executive forum on cybersecurity and were pleased the Food and Drug Administration has prioritized medical device security. The two also cited the "growing ability" of HHS' Critical Infrastructure Protection Division and the Health Sector Cybersecurity Coordination Center "to explain cyber threats through a sector-focused lens." However, they said they remain concerned "about the lack of robust and timely sharing of actionable threat information with industry partners and the need to dramatically scale up the Department's capabilities and resources." King and Gallagher asked Becerra to provide an assessment of the current organizational structure and roles and responsibilities HHS employs to support health care cybersecurity. They also asked Becerra to detail any gaps in current authorities HHS has to improve health care cybersecurity and the resources—including personnel and budget—that HHS requires to serve as an effective sector risk management agency.[4]

[1] American Medical Association, *Patient Perspectives Around Data Privacy*, July 25, 2022, https://bit.ly/3TspSVe.
[2] Cynerio report, *The Insecurity of Connected Devices in Healthcare* 2022, August 2022, https://bit.ly/3KzrGYg.
[3] David Mekeel, "Phoenixville Hospital Employee Fired After Improperly Viewing Patients' Medical Records," *Reading Eagle*, July 8, 2022, https://bit.ly/3CJCAJh.
[4] Angus King and Mike Gallagher, letter to Health & Human Services Secretary Xavier Becerra, August 11, 2022, https://bit.ly/3Rke6dv.