COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 3. March 11, 2021 Privacy Briefs: March 2021

By Jane Anderson

◆ **The Cybersecurity & Infrastructure Security Agency (CISA) has issued an emergency directive addressing critical vulnerabilities in Microsoft Exchange products.**[1] Successful exploitation of these vulnerabilities allows an unauthenticated attacker to execute arbitrary code on vulnerable Exchange servers. This could allow hackers to gain persistent system access and control of an enterprise network, CISA said. CISA and its partners have observed widespread active domestic and international exploitation of this vulnerability. CISA strongly recommends organizations examine their systems to detect any malicious activity detailed in its alert AA21-062A.[2] Microsoft has released an updated script that scans Exchange log files for indicators of compromise associated with the vulnerabilities.[3]

◆ **Health information of some University of Pittsburgh Medical Center St. Margaret hospital patients might have been "inappropriately disclosed" after an employee sent a medication administration report to an outside organization without a business need, UPMC officials said.** Officials at the 249-bed acute care and teaching hospital located in Pennsylvania said in a news release that they learned of the breach on Aug. 8.[4] Through an investigation, officials determined that names, internal UPMC identification numbers and medication administration data, such as drug name, dosage, date and time of administration, and reason for administration, may have been disclosed. Officials terminated the unnamed employee's access to UPMC systems, and the person is no longer affiliated with UPMC.[5]

◆ **Cloud security company Bitglass found that there were 599 health care breaches in 2020, a 55.1% increase since 2019, according to the firm's *Healthcare Breach Report 2021*.**[6] Hacking and information technology (IT) incidents were the top breach causes in health care in 2020, leading to 67.3% of compromises, the report said. Other breach causes included unauthorized disclosure (21.5% of breaches), and loss or theft (8.7% of breaches). "Breaches caused by hacking and IT incidents exposed 91.2% of all breached records in healthcare in 2020—24.1 million out of 26.4 million," the report said. "These results demonstrate the heightened impact of cybersecurity breaches, the shifting strategies of malicious actors, as well as how healthcare organizations are grappling with cybersecurity in today's dynamic, cloud-first world." As recently as 2014, lost and stolen devices were the leading causes of security breaches in health care, while hacking and IT incidents were the least common causes, the report said. "Today, things have essentially inverted. Hacking and IT incidents are now the primary forces behind healthcare breaches—as they have been each year since 2017. As organizations continue to embrace cloud migration and digital transformation, healthcare organizations must leverage the proper tools and strategies to successfully protect patient records and respond to the growing volume of threats to their IT ecosystems," the report said. The average cost per breached record increased from $429 in 2019 to $499 in 2020, and in 2020, the average health care firm took about 236 days to recover from a breach, according to the report.