# Report on Patient Privacy Volume 24, Number 4. April 11, 2024 Privacy Briefs: April 2024

By Jane Anderson

◆ **The Cybersecurity and Infrastructure Agency (CISA) is seeking comment on a proposed rule to implement reporting requirements for critical infrastructure entities, including health care entities, on cyberattacks and ransomware payments**. Congress mandated the rule in the Cyber Incident Reporting for Critical Infrastructure Act of 2022. It would require entities to report "substantial" cyber incidents to CISA within 72 hours and ransom payments within 24 hours. CISA defines "substantial" cyber incidents to include those that have any of these characteristics: (1) a loss of confidentiality, integrity or availability of an entity's information system or network; (2) a serious impact on the safety and resiliency of an entity's operational systems and processes; (3) a disruption of an entity's ability to engage in business or industrial operations or deliver goods and services; or (4) unauthorized access to an entity's information system or network, any nonpublic information contained in the information system or network that was facilitated through or caused by either a compromised of a cloud service provider, managed service provider, other third-party data hosting provider or a supply chain compromise. CISA said the rule would enhance its ability to spot trends in cyberattacks, help victims and quickly share information with other entities. The deadline for comments is June 3.[1]

◆ **Indiana Attorney General Todd Rokita has sued home health care provider Apria Healthcare LLC for violating HIPAA as a result of two data breaches two years apart that impacted 1.8 million people, including 42,000 Indiana residents**. Apria provides home health care equipment and related services to more than 2 million patients across 270 locations. According to Rokita's lawsuit, bad actors first gained access to Apria's environment in April 2019 and gained access a second time in August 2021. The FBI notified Apria on Sept. 1, 2021, that an unauthorized third party likely was able to access its system. "The intruder accessed millions of documents containing protected health information and other personal information," Rokita said. "Further, the intruder accessed several Apria employee email accounts, including Apria's CEO." At the time of the attack, Apria did not have two-factor or multi-factor authentication in place, the lawsuit said. According to Rokita, the breach involved Social Security numbers, birth certificates, credit and debit card information, medical histories, addresses and other information. In addition, Rokita said Apria failed to notify patients until May 2023, even though Apria's parent company—Virginia-based Owens & Minor— knew about the problem when it purchased Apria in March 2022.[2]