Report on Patient Privacy Volume 24, Number 2. February 08, 2024 Privacy Briefs: February 2024

By Jane Anderson

◆ **The American Hospital Association (AHA) has warned that information technology (IT) help desks are being targeted in a social engineering scheme that uses the stolen identity of revenue cycle employees or employees in other sensitive financial roles**. According to the AHA, the scheme is presumably a foreign-based threat actor calling IT help desks and leveraging stolen personally identifiable information of employees to answer security questions posted by the IT help desk. The threat actor then requests a password reset and requests to enroll a new device, such as a cell phone, to receive multi-factor authentication (MFA) codes, the AHA said, noting that the new device often will have a local area code. "This effectively defeats multi-factor authentication, including SMS text and higher level 'phishing-resistant' MFA, to provide full access to the compromised employee's email account and other applications," the AHA said. "The threat actor has reportedly used the compromised employee's email account to change payment instructions with payment processors and divert legitimate payments to fraudulent U.S. bank accounts. As with other payment diversion schemes, it is believed the funds are ultimately transferred overseas." The risk of this "innovative and sophisticated scheme" can be mitigated by ensuring strict IT help desk protocols, which at a minimum should require a call back to the number on record for the employee requesting password resets and enrollment of new devices, said John Riggi, AHA's national advisor for cybersecurity and risk. "Organizations may also want to contact the supervisor on record of the employee making such a request. As a result of becoming a victim of this scheme, one large health system now requires employees making such requests to appear in person at the IT help desk," Riggi said, adding that any organization that falls victim to a payment diversion scheme should notify their financial institution and the FBI.[1]