COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 4. April 06, 2023 Security Experts Warn of Threats from AI Phishing and Blockchain Data Compromise

By Jane Anderson

Most health care organizations understand the threats to protected health information (PHI) posed by lost laptops and rogue employees. But new dangers lurk alongside these old ones, in forms such as phishing powered by artificial intelligence (AI) and consumer-grade apps designed mainly for amusement, security experts say.

To counter these new types of threats, five experts interviewed by *Report on Patient Privacy* advised tried-and-true security tactics, such as performing thorough risk assessments and investing in comprehensive training. In addition, some recommended considering more advanced practices, such as automating incident response and moving to continuous risk assessment.

"Who really knows what the next big threat will be?" said David Harlow, chief compliance and privacy officer at Insulet Corporation. "The threats we continue to face are problematic because they are new, because they are unexpected. To quote Yogi Berra, 'It is hard to make predictions, especially about the future.' The best we can do is to continue to deploy zero-trust solutions and train people—and machines—to recognize attacks."

The commercialization of AI has been top-of-mind recently, exemplified by considerable interest and buzz in the news in recent weeks surrounding OpenAI's ChatGPT model, Alphabet Inc.'s DeepMind and Meta's quickly withdrawn language model Galactica, Harlow said.

He said this "demonstrates the power and the limitations—and the built-in risks—of any new technology, magnified by the way the chat outputs come across: seemingly authoritative and natural-sounding in the case of AI-generated text. Why is this a security issue? Well, to give one example: In the hands of a social engineering troll farm or ransomware-as-a-service developer, these sorts of tools are likely to make attacks more successful."

In fact, the HHS Health Sector Cybersecurity Coordination Center (HC3) warned in January that AI has evolved to a point where threat actors can use it to develop malware and phishing lures. Unfortunately, this threat will only get worse as the technologies improve, HC3 said. [1]

Rebecca Herold, president of SIMBUS360.com and CEO of The Privacy Professor, agreed that AI poses some threats within health care applications. "While AI brings some great, promising outcomes to find cures for diseases . . . AI can be used on databases that have been 'de-identified' to re-identify the associated individuals. The data could then be used in ways that could harm the individuals, and not to mention, to result in a breach for which the CE [covered entity] and/or the involved BAs [business associates] would be responsible," Herold said.