Report on Patient Privacy Volume 24, Number 1. January 11, 2024 Privacy Briefs: January 2024

By Jane Anderson

◆ **New York has released proposed cybersecurity regulations for hospitals. The regulations, which were published in *The State Register* on Dec. 6 and will undergo a 60-day public comment period ending on Feb. 5, are designed to help hospitals protect critical systems from cyber threats, state officials said**. Under the proposed regulations, hospitals will be required to establish a cybersecurity program and take steps to assess internal and external cybersecurity risks, use defensive techniques and infrastructure, implement measures to protect their information systems from unauthorized access or other malicious acts and take actions to prevent cybersecurity events before they happen, according to the state. In addition, the proposed regulations will require that hospitals develop response plans for a potential cybersecurity incident, including notification "to appropriate parties," and to run tests of their response plans to ensure that patient care continues while systems are restored. Once the regulations are finalized, hospitals will have one year to comply. New York Gov. Kathy Hochul's 2024 budget includes $500 million in funding for health care facilities to upgrade their technology systems to comply with the proposed regulations.[1]

◆ **Some patients of Oklahoma City-based Integris Health were contacted in December by apparent hackers who claimed to have stolen their personal information and threatened to post it on the dark web**. An email shared on social media, allegedly from the hackers, stated that the attackers obtained names, contact information, work and insurance information, plus Social Security numbers. "We have contacted Integris Health, but they refuse to resolve this issue," the email stated. The alleged hackers also said that if the email recipient did not pay a ransom of $50 in Bitcoin, their information would be sold to data brokers on the dark web. In a privacy notice dated Dec. 24, Integris Health said that it became aware of the breach on Nov. 28. The hospital system said that names, dates of birth, contact information, demographic information and Social Security numbers were included in the breach. Payment information, such as credit card numbers, usernames or passwords and driver's license numbers or other government-issued identification were not included in the breach, Integris said. The hospital system urged patients not to respond to emails from the apparent hackers or to "follow any of the instructions, including accessing any links."[2]