COSMOS
Navigate the Compliance Universe

# Report on Patient Privacy Volume 20, Number 1. January 09, 2020 Health Care Needs to Play Catch-Up Fast to Address New 2020 Threats, Experts Say

By Jane Anderson

Ransomware and phishing attacks will target the most vulnerable health care entities specifically as 2020 gets underway, and many organizations lag well behind in addressing key weaknesses in both their information technology (IT) systems and in their training, cybersecurity experts say.

As the volume of data expands and brand-new interconnected Internet-of-Things (IoT) health care devices come online, experts tell *RPP* that organizations need to stress the basics in security: patching; training; and accurate, thorough data mapping. At the same time, organizations should expect ramped up enforcement activities from states, particularly California, experts say.

The expected security threats this year are predictable based on those incidents that occurred in 2019, says Michelle O'Neill, director of corporate compliance at Summit Health Management in New Jersey.

"The most common attacks include phishing, social engineering, medical device security, legacy operating system flaws, malware and ransomware. Ransomware will most likely remain at the top of the list—consistent with 2019—but it looks like ransomware will continue to evolve and primarily focus on the cloud. Lateral phishing attacks are also predicted to rapidly increase," O'Neill says. "As far as differences [from 2019] go, medical device security has taken some of the spotlight, in addition to legacy [operating system] flaws, which is a fairly new concept in the cybersecurity world."