COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 8. August 06, 2020 Hit with Ransomware? Here's What Your Organization Is Up Against

By Jane Anderson

Ransomware attacks are changing and becoming far more sophisticated, meaning hospitals and other health care entities need to step up their games to defend against these potentially crippling security events, the American Hospital Association (AHA) concluded.[1]

"The threat I worry most about is a ransomware attack on an overloaded hospital caring for COVID-19 patients that would interrupt patient care, or worse, shut down operations at the facility—thereby putting frail patient lives at risk," wrote John Riggi, AHA senior advisor for cybersecurity and risk. Riggi pointed out that a ransomware attack in the Czech Republic resulted in that exact outcome, with Brno University Hospital forced to redirect patients to other hospitals.

Most cyberattacks on health care facilities are carried out by skilled, sophisticated criminal groups, Riggi said, and therefore, hospitals need to work with federal investigators and coordinate among themselves. "Leveraging the entire law enforcement, intelligence and military capabilities of the U.S. government is necessary to achieve swift and certain consequences against these attackers," he added in the document authored for AHA members.