COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 30, Number 9. March 08, 2021
OFAC Fines Add to Ransomware Peril; 'It's a Between-a-Rock-and-a-Hard-Place Thing'

By Nina Youngstrom

Organizations have been warned by the U.S. Office of Foreign Assets Control (OFAC) that they may be fined if they pay ransom to "malicious cyber actors" to unlock their information systems. That complicates the decision whether to pay when attacked by ransomware and its variant, distributed denial of service (DDoS). Health systems should incorporate OFAC penalties into their prepayment due diligence and cybersecurity programs, attorneys said. They may pay the ransom anyway but will do it with their eyes open. This adds another dimension to ransomware at a time when the number of attacks is rising and cybercriminals may use artificial intelligence to make a bad situation worse.

In an Oct. 1 advisory,[1] OFAC stated that organizations are subject to fines if they paid ransom to people or entities on its "Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria)." That puts hospitals and health systems in a difficult position because they need to regain access to their protected health information (PHI) and business records immediately, especially if threat actors have hijacked their backup systems.

"It's a between-a-rock-and-a-hard-place thing," said Dave Summitt, chief information security officer at Moffitt Cancer Center in Tampa, Florida. "You may not have a choice to pay the ransom and make a recovery." But now hospitals must consider the risks in the advisory from OFAC, which is part of the Treasury Department, and "pull OFAC into their overall cyber preparedness and response plan," said David Rybicki, former deputy assistant attorney general. "Treasury wants to send a message you can face liability and will expect internal controls that are OFAC specific and pressure tested," said Rybicki, now an attorney with K&L Gates in Washington, D.C.

The OFAC advisory said there was a 37% increase in ransomware attacks from 2018 to 2019. "Our systems detect a ransomware attempt probably every week, three to four times," Summitt said. They're costing organizations a fortune, whether or not they pay the ransom. A cyberattack cost Universal Health Services, a huge hospital chain, $67 million in pre-tax losses, according to CyberScoop.[2] A Sept. 27 breach led to delayed billing, diversion of ambulances to competitors and spending on labor to restore connectivity.

The OFAC advisory said it could levy civil penalties on organizations for violations based on strict liability, which means they can be fined even if they didn't know they were engaging in a transaction with a person or entity on the SDN List.