COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 30, Number 44. December 13, 2021
Whether to Pay Ransom is Tricky Decision, But Few Get Data Back

By Nina Youngstrom

When organizations are hit with a ransomware attack, they're faced with a series of agonizing decisions that are getting more difficult to make as the cyber mafia operates more like a business yet isn't reliable. Even if organizations pay the ransom, they're unlikely to get back their data and may invite more attacks, and there's a risk of penalties from the Office of Foreign Assets Control (OFAC),[1] experts say.

"It is getting tougher to manage ransomware incidents, and they have increased so significantly," said Phyllis Sumner, an attorney with King & Spalding and its chief privacy officer.

Only 8% of businesses retrieved their data after forking over money to cyber criminals in a ransomware attack, Sumner said.[2] "Even if you pay for the decryption keys, very few organizations successfully get their data back," she said. "The misperception can be that it's easier or effective to pay the ransom and you simply decrypt your files. It's rarely the case an organization gets all their data back. That's something to weigh in the risk analysis when thinking about whether to pay the threat actor." Organizations instead may pay threat actors for their promise not to sell or post the data, but they're criminals, and their word isn't exactly their bond. Either way, health care organizations still must abide by breach notification requirements.