COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 31, Number 38. October 17, 2022
Feds Discourage Ransom Payments, but 'the Answer Is Not That Simple'

By Nina Youngstrom

The government discourages paying ransom to cybercriminals and in some cases prohibits it, but health care organizations may decide it's worth making a dubious deal with the devil to try to get back their data or keep it off the dark web, attorneys say. If they go that route, organizations run the risk of sanctions from the Treasury Department and will soon face new reporting requirements. They should look to the HIPAA security rule for cybersecurity preparedness, especially with the new Department of Justice (DOJ) civil cyber-fraud initiative, although HIPAA faces criticism for not keeping up with technology advances.

The FBI, the Cybersecurity and Infrastructure Security Agency (CISA) and the Treasury Department "all discourage paying ransom with the understanding by doing so there is no guarantee you will get files back and there can be sanctions risk in some situations," said attorney Kate Driscoll, with Morrison Foerster, at a Sept. 20 webinar sponsored by the Health Care Compliance Association. Treasury's Office of Foreign Assets Control (OFAC) issued an updated advisory in September 2021 on "sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks."[1] It's a carrot-stick approach, she noted. As OFAC explained, "U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ('persons') on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes."