COSMOS
Navigate the Compliance Universe

# Report on Medicare Compliance Volume 31, Number 10. March 21, 2022
# New Law Requires Disclosure of Ransomware Payments; CMS Plans Outreach on End of PHE

By Nina Youngstrom

Cybersecurity incidents and ransomware payments must be disclosed to a component of the Department of Homeland Security (DHS), according to a provision in the 2022 Consolidated Appropriations Act (CAA), the $1.5 trillion budget bill signed into law by President Biden March 15.[1] It's the same law that extends Medicare telehealth flexibilities for five months after the end of the COVID-19 public health emergency (PHE).[2]

"This would require hospitals to report cyber breaches in 72 hours and any ransomware payments made in 24 hours to DHS," said Kim Brandt, former principal deputy administrator for operations and policy at CMS and a former Senate counsel, at the Health Care Compliance Association's virtual regional conference March 11.[3] "This is really important because it is an additional reporting burden" for covered entities, which already have HIPAA breach reporting obligations. Brandt also gave other updates related to the legislation, the PHE and Medicare payment rules.

According to the CAA, critical infrastructure sectors, including hospitals and health systems, will report cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA) at DHS. But they have time to think about compliance, said Barry Mathis, consulting principal with PYA. The legislation gives CISA 24 months to propose implementing regulations, which must be finalized 18 months later, he said. "This is not something covered entities have to run out and do tomorrow. However, it is possible CISA may move faster based on recent concerns about Russian cyberattacks."

The regulations will define covered entities based on a number of factors, including "the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety," according to the law. The regulations also will explain what information must be included in reports submitted to CISA, although the legislation already specifies a description of the ransomware attack; "vulnerabilities, tactics, techniques, and procedures used to perpetrate the ransomware attack;" the amount of ransom paid and when; and ransom payment instructions, among other things.