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.

Although the legislation is the government's attempt to get a better fix on the prevalence of ransomware payments, mandatory reporting runs counter to the culture at many organizations, Mathis said. "The knee-jerk reaction at most hospitals is, 'Let's keep this quiet.'" They hope to deal with the cybercriminal version of a "reputable" hacker—paying the ransom, unlocking their data and keeping it off the dark web. But the federal government is "stepping in and saying it's tired of people paying ransom," which the FBI believes has "created an epidemic of ransomware attacks," Mathis said. "If bad actors get paid, it's a business for them." He noted the legislation doesn't forbid ransom payments, although 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.[4]

The secrets that covered entities must spill about some of their cyber incidents won't be available to the public,

Mathis said. The reports to CISA can't be obtained through the Freedom of Information Act or used for other regulatory purposes (e.g., enforcement by the HHS Office for Civil Rights), he said. They will be treated as proprietary information.

Mathis noted the legislation was "something the cyber infrastructure folks have been talking about for a while." It isn't a response to potential Russian cyberattacks as a result of sanctions related to the war in Ukraine or any specific event, he said, although on March 15, CISA and the FBI released a joint advisory warning "that Russian state-sponsored cyber actors have gained network access through exploitation of default [multifactor authentication] protocols and a known vulnerability" ("PrintNightmare").[5]

CMS Is Planning Outreach Before End of PHE

The CAA also extends Medicare coverage of telehealth services that are products of the PHE and its waivers for 151 days after the end of the PHE, including audio-only telehealth and other flexibilities. Perhaps the broadest stroke is the bill's definition of "originating site" to mean any site where an "eligible telehealth individual is located" when services are performed. Before the PHE, the originating site requirement generally restricted Medicare coverage to services delivered to patients at hospitals and other provider locations (not patient homes) by distant site practitioners (e.g., physicians). The COVID-19 waivers set aside the originating site requirement for telehealth services, allowing them to be delivered in patient homes. The legislation appears to be even more far-reaching than the waivers, allowing Medicare coverage of telehealth services delivered anywhere the patient is (e.g., a coffee shop, the patient's car, a library).The CAA also allows telehealth services to continue to be provided anywhere in the country for 151 days after the PHE ends, not just rural areas.

The PHE ends April 15, but "everyone's assumption is it will be extended for another 90 days," said Brandt, a partner in Tarplin, Downs & Young. By statute it must be extended in 90-day increments, so HHS couldn't terminate another extension early, which would take the PHE through mid-July. After the PHE ends, every flexibility and waiver, including Acute Hospital Care at Home, alternate sites of service, documentation relaxation and many others, "end at midnight on the day the PHE expires," she said, except for telehealth.

But CMS has a soft landing in mind. It's "already planning education and outreach for providers to ensure there is ample lead time for them to prepare before the end of the PHE," Brandt said. HHS Sec. Xavier Becerra, CMS Administrator Chiquita Brooks-LaSure and others have said they intend to give providers a 60-day notice that the PHE will be over.

Even with a runway, there's no escaping the challenges it presents for health care organizations to revert to billing, documentation, licensure and other pre-PHE practices. "This is a huge compliance nightmare depending how much you have been using flexibilities," Brandt noted. "CMS's contractors and their colleagues at the HHS Office of Inspector General will be doing tons of post-pandemic oversight to ensure providers haven't gamed the system and don't do it after [the PHE]. It's something you have to be super vigilant about."

More Emphasis on Health Equity

There were other health care provisions in the CAA. For example, Congress protected certain 340B hospitals that lost their eligibility because a dip in their disproportionate share hospital adjustment percentage put them below the threshold for 340B eligibility, Brandt said. They gained "limited access to the program."

Brandt said providers should expect far more emphasis on health equity and value-based care during the Biden administration. For example, Part A payment regulations that are at the Office of Management and Budget for review have a heath equity component and focus on value-based care. "Equity in health outcomes remains a top priority for the administration and Congress, driven by the pandemic's disproportionate impact on low-income

and historically marginalized groups," she said.

Also, the Center for Medicare & Medicaid Innovation (CMMI) has "made it clear they want all Medicare beneficiaries and the vast majority of Medicaid beneficiaries in an accountable care relationship with a provider by 2030. The current strategy released by CMMI indicates that new models will be simpler, fewer and mandatory. They have been publicly supportive of direct contracting and making improvements to that program. However, pushback from House Democrats of the direct contracting program will be an area to watch depending on how much traction that effort gains."

Contact Mathis at bmathis@pyapc.com and Brandt at kbrandt@tyllc.com.

1 Consolidated Appropriations Act, H.R. 2471 (2022), https://bit.ly/3KQWh2K.
2 Nina Youngstrom, "Congress Extends Telehealth Coverage for 151 Days After PHE; Patients May Be at Home," *Report on Medicare Compliance* 31, no. 9 (March 14, 2022), https://bit.ly/3CMtkCe.
3 Kimberly Brandt, "Healthcare Regulatory, Enforcement and Policy Issues," Washington, DC Regional Healthcare Compliance Conference, Health Care Compliance Association, March 11, 2022, https://bit.ly/3Ii0HOm.
4 Nina Youngstrom, "OFAC Fines Add to Ransomware Peril; 'It's a Between-a-Rock-and-a-Hard-Place Thing,'" *Report on Medicare Compliance* 30, no. 9 (March 8, 2021), https://bit.ly/3fHpBMo.
5 Cybersecurity and Infrastructure Security Agency, "Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and 'PrintNightmare' Vulnerability," Alert (AA22-074A), March 15, 2022, https://bit.ly/3tX5YWg.