COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 33, Number 9. March 11, 2024
Change Healthcare Is Returning After Cyberattack; Things May Be Different for Future Victims

By Nina Youngstrom

The paradox of the Feb. 21 cyberattack on Change Healthcare is that it has shaken the health care world to its core but seems otherwise unremarkable in a technical sense, experts say. Although UnitedHealth Group, which owns Change Healthcare, said March 7 that so far its electronic prescription platform is back, the clearinghouse has already been shut down for two weeks, affecting electronic claims processing, insurance verification and remittance advices for many hospitals and other providers.[1] That led to intervention from HHS and CMS, which opened the door to accelerated Medicare payments and relaxed Medicare Advantage prior authorization requirements. At the same time, the FBI's quick disruption of the threat actors or their own infighting may change the landscape for future victims of ransomware attacks.

"We can't overstate the impact on the entire health care industry," said Hillary Harlan, a senior manager at Stout, a global advisory firm. HHS announced March 5 that Medicare providers that need to switch clearinghouses should contact their Medicare administrative contractor (MAC) to ask for a new electronic data interchange (EDI) enrollment.[2] CMS has asked MACs to speed up the process.

Change Healthcare confirmed it "experienced a cybersecurity issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat." The situation has apparently just taken a turn for the better, however, according to UnitedHealth Group, which also announced that Change Healthcare's electronic payments platform will be available March 15. UnitedHealth anticipates testing and reestablishing connectivity to the claims network and software March 18, with service restored through that week. There's no word on how it's recovering the systems.

Although the Change Healthcare ransomware attack was "big and very visible and has the most impact, it feels like business to me," said Nathan Ruehs, director of the cybersecurity division at N1 Discovery. "The big disruption is the change we have seen in the FBI response. For victims who think the normal process is, 'I have all the time in the world to talk to these guys, maybe we'll pay them,'" that's not how things played out with Change Healthcare and there are implications for other organizations that are hit with ransomware attacks. With Change Healthcare, the FBI apparently moved in quickly. "It's a good thing they disrupted it so fast," Ruehs said. "It makes the threat actors less stable." Change Healthcare reportedly paid the main threat actor a ransom of $22 million but the main threat actor didn't share the money with its affiliate, as supposedly promised.[3] "Now the threat actors are lashing out in unpredictable ways," and that may affect how hospitals and other victims respond to ransomware attacks.