Report on Patient Privacy Volume 21, Number 5. May 06, 2021 Stark Rules Now Allow Donations of Security Equipment, Services

By Jane Anderson

Long sought-after changes in the anti-kickback physician self-referral regulations now allow large health care entities, such as health systems, to donate cybersecurity equipment and services to smaller entities, such as physician practices, in an effort to strengthen those practices against cyberattacks.

The rules, issued late last year by the HHS Office of Inspector General (OIG) and the Centers for Medicare & Medicaid Services (CMS), implement changes to the Stark physician self-referral law and to related anti-kickback regulations.[1]

The rules establish "a safe harbor or an exception to each of these regulatory constructs that is intended to allow for the donation of technology and services for cybersecurity," said David Holtzman, principal consultant at HITprivacy LLC. These rules are "intended to be broad in scope, with the stated intent of being protective of arrangements that are intended to address the growing threat of cyberattacks that are impacting the health ecosystem," Holtzman told attendees during a recent session at the 30th annual National HIPAA Summit, which was held virtually.[2]

Under the safe harbor and Stark Law exception, "larger health care providers will now be able to provide other health care providers, such as individual physician practices, with cybersecurity solutions and donations, as long as certain requirements that protect against fraud and abuse are met," Holtzman explained. "Through the new safe harbor and Stark exception, HHS seeks to promote the use and donation of cybersecurity technology, which in turn should result in a more robust cybersecurity framework for the entire health care industry."