von Briesen
von Briesen & Roper, s.c. | Attorneys at Law

Offered Free Cyber Services? You May Not Need to Look That Gift Horse in the Mouth Any Longer.

Jan 20 2020

Practice Area: Health Law & Information Technology, Data Privacy and Security & Health Information Privacy and Security

Cyberattacks continue to plague health care entities. In an effort to promote improved cybersecurity and prevent those attacks, HHS has proposed new rules under Stark and the Anti-Kickback Statute ("AKS") to protect in-kind donations of cybersecurity technology and related services from hospitals to physician groups. There is already an EHR exception[1] which protects certain donations of software, information technology and training associated with (and closely related to) an EHR, and HHS is now clarifying that this existing exception has always been available to protect certain cybersecurity software and services. However, the new proposed rule explicitly addresses cybersecurity and is designed to be more permissive then the existing EHR protection.

The proposed exception under Stark and safe harbor under AKS are substantially similar and unless noted, the following analysis applies to both. The proposed rules allow for the donation of cybersecurity technology such as malware prevention and encryption software. The donation of hardware is not currently contemplated, but HHS is soliciting comment on this matter as discussed below. Specifically, the proposed rules also allow for the donation of cybersecurity services that are necessary to implement and maintain cybersecurity of the recipient's systems. Such services could include:

- Services associated with developing, installing, and updating cybersecurity software;
- Cybersecurity training, including breach response, troubleshooting and general "help desk" services;
- Business continuity and data recovery services;
- "Cybersecurity as a service" models that rely on a third-party service provider to manage, monitor, or operate cybersecurity of a recipient;
- Services associated with performing a cybersecurity risk assessment or analysis, vulnerability analysis, or penetration test; or
- Services associated with sharing information about known cyber threats, and assisting recipients responding to threats or attacks on their systems.

The intent of these rules is to allow the donation of these cybersecurity technology and services in order to encourage its proliferation throughout the health care community, and especially with providers who may not be able to afford to undertake such efforts on their own. Therefore, these rules are expressly intended to be less restrictive than the previous EHR exception and safe harbor. The proposed restrictions are as follows[2]:

- The donation must be necessary to implement, maintain, or reestablish cybersecurity;
- The donor cannot condition the donations on the making of referrals by the recipient, and the making of referrals by the recipient cannot be conditioned on receiving a donation; and
- The donation arrangement must be documented in writing.

AKS has an additional requirement that the donor must not shift the costs of any technology or services to a Federal health care program. Currently, there are no "deeming provisions" within these proposed rules for the purpose of meeting the necessity requirement, but HHS is considering, and is seeking comment on, whether to add deeming provisions which essentially designate certain arrangements as acceptable. Some in the industry appreciate the safety of knowing what is expressly considered acceptable and others find this approach more restrictive out of fears that the list comes to be considered exhaustive.

HHS is also considering adding a restriction regarding what types of entities are eligible for the donation. Previously for other rules, HHS has distinguished between entities with direct and primary patient care relationships, such as hospitals and physician practices, and suppliers of ancillary services, such as laboratories and device manufacturers.

Additionally, HHS is soliciting comment on whether to allow the donation of cybersecurity hardware to entities for which a risk assessment identifies a risk to the donor's cybersecurity. Under this potential rule, the recipient must also have a risk assessment stating that the hardware would reasonably address a threat.

---

[1] AKS Safe Harbor 42 CFR §1001.952(y); Stark Exception §411.357(bb)
[2] AKS Safe Harbor 42 CFR §1001.952(jj); Stark Exception §411.357(w)(4)
