HALL RENDER
KILLIAN HEATH & LYMAN

HEALTH INFORMATION TECHNOLOGY

OCTOBER 10, 2019

EHR DONATIONS AND CYBERSECURITY TECHNOLOGY EXCEPTION INCLUDED IN NEW PROPOSED RULES FROM OIG, CMS

On October 9, 2019, both the Health and Human Services Office of Inspector General ("OIG") and Centers for Medicare & Medicaid Services ("CMS") issued proposed rules pertaining to the Anti-Kickback Statute safe harbor and Civil Monetary Penalties Law exception for EHR Donations ("EHR Donation Rules"), as well as a new safe harbor and exception for cybersecurity technology and related services ("Cybersecurity Rules"). The proposed EHR Donation Rules will be welcome by those entities currently providing ongoing EHR donation programs as the current EHR Donation Rules were set to expire December 31, 2021. The proposed Cybersecurity Rules will give health care entities additional tools and opportunities to combat cyberattacks, including ransomware, through collaborative efforts.

EHR DONATION RULES

Sunset Date

The proposed EHR Donation Rules provide specific language to modify the existing rule, as well as request feedback on possible modification to the EHR Donation Rules beyond the new proposed language. The most noteworthy modification is the elimination of the sunset date, which is currently December 31, 2021. As you may recall, the original EHR Donation Rules issued, August 8, 2006, had an expiration date of December 31, 2013, and this expiration date was extended to December 31, 2021 by new regulations issued December 27, 2013. The proposal is to eliminate the expiration and make the EHR Donation Rules permanent.

Information Blocking

The proposed EHR Donation Rules double down on support of prohibitions on information blocking as legislated in the 21st Century Cures Act. First, the proposed EHR Donation Rules would change the definition of "interoperable." The proposed modification first defines "interoperable" so that the donated technology and services must be able to communicate and exchange data with and use data from other technology without special effort and must allow complete access, exchange and use in compliance with applicable laws. Finally, the proposed modifications would deem the donated technology and services to not be interoperable if such technology or services constitute information blocking under the 21st Century Cures Act provisions. In addition to the proposed modification of interoperable, the proposed EHR Donation Rules would delete the prior requirements that the donor not restrict or limit use or compatibility of the donated technology or services and replace it with a requirement that the donor not engage in a practice constituting information blocking under the 21st Century Cures Act.

Definition of Electronic Health Record

The proposed EHR Donation Rules also modify the definition of "electronic health record" in a manner which in our opinion broadens the scope of the exception and safe harbor. Previously, the definition of "electronic health record" required that the donated items and services related to technology "used for clinical diagnosis and treatment." The proposed EHR Donation Rules modify the definition to include any repository of electronic health information. In fact, the language proposed essentially paraphrases the definition of Protected Health Information found in HIPAA. Whether intended or not by the proposed EHR Donation Rules, this new definition would seemingly include any system that is a repository from which protected health information is transmitted or maintained.

Recipient Contributions

The proposed EHR Donation Rules are seeking comments as to the necessity of the recipient to contribute toward the cost of the donated EHR items and services. The current EHR Donation Rules require that the recipient of an EHR donation pay at least 15 percent of the donor's cost of the donated items or services. The purpose of this recipient contribution is to address concerns with fraud and abuse risks inherent in EHR donations. Because some commentators believe that the 15 percent contribution threshold is burdensome for small and rural providers and represent a barrier to EHR adoption, the proposed EHR Donation Rules are specifically seeking comments as to three possible modifications to the EHR Donation Rules: (1) elimination of the recipient contribution requirement for small and rural providers and how small and rural providers should be defined; (2) the complete elimination of the recipient contribution requirement; and/or (3) the elimination of the recipient contribution requirement for upgrades to previously donated EHR items or services.

Replacement Technology

Some commentators to the EHR Donation Rules believe that the requirement that the prohibitions on donations to replace equivalent technology results in EHR lock-ins that are conducive to good clinical practices. These commentators believe this prohibition has resulted in physicians continuing with the same "inadequate" EHR vendor because they are not eligible for a donation to replace their current EHR with a more "adequate" solution. The proposed EHR Donation Rules are seeking comments as to whether this equivalent technology prohibition should be eliminated, thus permitting donations for EHR items or services that are replacing existing EHR systems.

CYBERSECURITY RULES

The proposed Cybersecurity Rules would add a safe harbor for donations of cybersecurity technology and services. CMS and OIG express the position that a cybersecurity safe harbor could remove barriers to address cyberattacks targeted at health records. The interconnectedness of health care delivery systems means that an attack on a “weak link” in the interconnected ecosystem can have repercussions that impact other members of that same ecosystem. The proposed Cybersecurity Rules posit that donations of technology and services of value to physicians who are sources of federal health care program referrals may indeed pose increasing fraud and abuse risks, but the risk is similar to the risk of EHR donations. The value of cybersecurity technology or services ranges widely, from antivirus software at a work station to robust incident response services for a multitude of entities.

Cybersecurity is defined as “the process of protecting information by preventing, detecting, and responding to cyberattacks.” This definition is intentionally broad because the Cybersecurity Rules acknowledge that new technology may become available. Like the EHR Donation Rules, hardware is excluded even though it is relevant to cybersecurity, due to a perceived higher risk that hardware can bring benefits to recipients beyond use for cybersecurity purposes. The proposed Cybersecurity Rule does, however, solicit comments as to: (1) the inclusion of specific hardware that is stand-alone and necessary for cybersecurity and only serves cybersecurity purposes; and (2) an alternative approach that would allow for cybersecurity hardware donations, provided the hardware is determined by the donor to be reasonably necessary based on a risk assessment of both the donor and the potential recipient.

To ensure donations are addressing the legitimate cybersecurity needs of donors and recipients to prevent, detect and respond to cyberattacks, the proposed Cybersecurity Rule will be limited to only donated technology and services that are necessary and used predominantly to implement, maintain or reestablish cybersecurity. Technology would consist of “any software or other types of information technology, other than hardware.” Technology could include encryption filtering of email traffic and software that protects systems. Services are also broad and can include training, cybersecurity as service models, testing, analysis, business continuity and data recovery services. Donations of services must be non-monetary where, for example, consultant time is permitted but not money to pay for a ransom associated with a ransomware attack.

All donations of cybersecurity technology and services must be documented in a written agreement and neither the eligibility of recipients nor the amount or nature of the technology or services be determined in a manner that takes into account the volume or value of the recipient's referrals, or be conditioned on the recipient doing business with the donor. Costs of cybersecurity donations are not permitted to be shifted to federal health care programs. This means the cost of the donor’s own cybersecurity technology and services is an administrative expense that could be included in a cost report; however, donations would not be permitted to be included.

The commentary to the proposed Cybersecurity Rules emphasize that a donor could provide cybersecurity technology and services to those who connect to the donor’s systems. This would include entities and individuals that refer to or receive referrals from the donor. The donor is not, however, obligated to provide cybersecurity technology and services to any and every entity that connects to its system. In deciding which individuals and entities should receive donations of cybersecurity technology and services, the donor can establish criteria, as long as the criteria do not take into account the volume or value of referrals or other business generated between the parties. The proposed Cybersecurity Rules do not require specific selection criteria.

Donors

The proposed Cybersecurity Rules are soliciting comments as to whether particular types of individuals or entities should be excluded as donors of cybersecurity technology and services.

Recipients

Unlike the current EHR Donation Rules, a recipient contribution is not required for a cybersecurity donation. The proposed Cybersecurity Rules express a belief that quantifying, aggregating and allocating costs related to cybersecurity technology and services may be unworkable and thus a recipient contribution may be difficult or impossible to calculate. This does not mean that donors cannot require recipient contributions as part of their cybersecurity donation programs.

If you have any questions or would like additional information about this topic, please contact:

- Jeff Short at (317) 977-1413 or jshort@hallrender.com or your regular Hall Render attorney;
- Patricia Connelly at (317) 429-3654 or pconnelly@hallrender.com; or
- Your regular Hall Render attorney.

For more information on Hall Render's Health Information Technology services, click here.