OVERVIEW OF CMS' STARK AND OIG'S ANTI-KICKBACK PROPOSED RULES:

CYBERSECURITY DONATION EXCEPTION / SAFE HARBOR

(Jan. 2019)

On October 9, 2019 the U.S. Department of Health & Human Services (HHS) **published** two proposed rules that would allow donations of cyber technology, extend the period for EHR donations, and make changes intended to facilitate the pathway to value based care. Together, the rules:

- **Electronic Health Record (EHR) Donations**
  - **Expand EHR donation exception:** This would amend the EHR exception to clarify that the exception is available (and always has been available) to protect certain cybersecurity software and services, and to more broadly protect the donation of software and services related to cybersecurity. CHIME and AEHIS spearheaded the advocacy behind the cyber donations and are pleased HHS ultimately agreed to propose these important exceptions.
  - **Remove the EHR donation sunset:** The EHR donation exception is schedule to sunset on Dec. 31, 2021. Under these rules, the HER donation would continue in perpetuity.
- **Cybersecurity**
  - **Create a new cyber exception:** A new exception specifically tailored to protect arrangements involving the donation of cybersecurity technology and related services (the cybersecurity exception). As proposed, the cybersecurity exception is broader and includes fewer requirements than the EHR exception. The predominant purpose of the software or services must be cybersecurity associated with the EHR. A party seeking to protect an arrangement involving the donation of cybersecurity software and services only needs to comply with the requirements of one applicable exception.

- **Value-based Care**
  - **Multiple changes intended to facilitate value-based care:** Among many of these proposed policies, the Administration calls for three proposed new safe harbors for certain remuneration exchanged between or among participants in a value-based arrangement (as further defined) that fosters better coordinated and managed patient care including:
    - Care coordination arrangements to improve quality, health outcomes and efficiency;
    - Value-based arrangements with substantial downside financial risk; and
    - Value-based arrangements with full financial risk. These proposed safe harbors vary, among other ways, by the types of remuneration protected (in-kind or in-kind and monetary) and the level of financial risk.
- **The links for the rules and fact sheets are below (NOTE: The rules are only in proposed form. None of the changes proposed are effective unless adopted in final rules)**
  - **OIG rule** and **fact sheet**
  - **CMS rule** and **fact sheet**

Cybersecurity Donation	OIG	CMS	AGENCY DISCUSSION / JUSTIFICATION
Excludes Hardware	✓	✓	• More likely to be "multi-purpose" (i.e. laptop donation would be prohibited but encryption software for laptop is ok) • Higher risk of fraud and abuse because could induce referrals
Excludes multi-purpose software	✓	✓	
Examples of protected software (includes but is not limited to…)	✓		• Software that provides malware prevention • Software security measures to protect endpoints that allow for network access control • Business continuity software that mitigates the effect of cyberattacks • Data protection and encryption • email traffic filtering
Monetary donations prohibited	✓	✓	• Paying ransomware is prohibited
Definitions:			
Cybersecurity	✓	✓	OIG "Cybersecurity" means the process of protecting information by preventing, detecting, and responding to cyberattacks. CMS The process of protecting information by preventing, detecting, and responding to cyberattacks. • Applies both to this safe harbor and the HER donation one
Technology	✓	✓	OIG "Technology" means any software or other types of information technology, other than hardware. CMS To mean any software or other type of information technology other than hardware. • This definition only applies to cyber safe harbor
No restrictions on types of donors	✓	✓	• CMS is considering limiting who can donate and seek comments on this.

			• CMS says in past rulemakings they have distinguished between individuals and entities with direct and primary patient care relationships that have a central role in the health care delivery infrastructure, such as hospitals and physician practices, and suppliers of ancillary services, such as laboratories, and manufacturers or vendors that indirectly furnish items and services used in the care of patients.
Recipients cannot condition receipt of tech/services on referrals	✓	✓	
Services (include but are not limited to…)	✓	✓	• Any services associated with developing, installing, and updating cybersecurity software; • Any kind of cybersecurity training services, such as training recipients on how to use the cybersecurity technology, how to prevent, detect, and respond to cyber threats, and how to troubleshoot problems with the cybersecurity technology (e.g., "help desk" services specific to cybersecurity); • Any kind of cybersecurity services for business continuity and data recovery services to ensure the recipient's operations can continue during and after a cyberattack; • Any kind of "cybersecurity as a service" model that relies on a third-party service provider to manage, monitor, or operate cybersecurity of a recipient; • Any services associated with performing a cybersecurity risk assessment or analysis, vulnerability analysis, or penetration test; or • Any services associated with sharing information about known cyber threats, and assisting recipients responding to threats or attacks on their systems.
Installation, improvement, or repairs related to physical safeguards NOT included	✓	✓	• Too valuable and could reduce referrals
Required cost-sharing with recipient	$0	$0	• Many providers under-resourced • Will free up more resources for recipients to invest in their own hardware • OIG says its also hard to quantify the value of cyber tech
Five Conditions must be met for safe harbor to apply	✓		• Permitting limited donations of certain hardware • Would be limited to "stand-alone" hardware; cannot be "integrated" into "multi-functional" equipment • Example given is two-factor authentication dongle • 5 conditions must be met to qualify:

			1. Are technology and services that are necessary and used predominantly to implement and maintain effective cybersecurity. 2. Donor cannot require, explicitly or implicitly, that a recipient either refer to the donor or recommend the donor's business as a condition of receiving a cybersecurity donation. 3. Recipients / potential recipients prohibited from demanding cyber tech or services on conditions of referrals or doing business 4. Donors and recipients must enter into a written agreement 5. Prohibition on cost shifting

Recipient selection		✓	• CMS says there are two ways a donor could decide which recipients to donate to:
			  ○ Perform risk assessment of a potential recipient (or require them to perform it); or
			  ○ Donor can select recipients based on the type of actual or proposed interface between them

Deeming provision	✓	✓	• Considering deeming provision that would allow donors or recipients to demonstrate that donations are necessary and predominantly used to implement and maintain cybersecurity • Would allow donors and recipients to demonstrate donation furthers a recipient's ability to comply with a written cybersecurity program that reasonably conforms to a widely recognized cybersecurity framework or set of standards, such as one developed or endorsed by NIST, another American National Standards Institute-accredited standards body, or an international voluntary standards body such as the International Organization for Standardization. • Would not require compliance with any particular framework – instead would provide an option for donors to demonstrate that the donation is necessary and predominantly used to implement and maintain effective cybersecurity. • CMS did say they are worried deeming provisions pertaining to the volume or value of referrals or other business generated may be interpreted as prescriptive requirements
List of criteria that do not implicate volume or value	✓	✓	• Feels cyber donations do not pose a risk like EHR donations to volume or value of referrals • Offers no list but CMS & OIG says they are considering one
Donors	✓		• No restrictions on which entities can donate • OIG includes patients as among the protected recipients and they anticipate donations to them would be more limited • Donations do not need to solely occur between 2 parties (i.e. 2 providers can jointly subsidize a small practice)
Conditions on Donation and Protected Donors		✓	• Proposing to limit the applicability of the exception for cybersecurity technology and related services to donated technology or services that are necessary and predominantly used to implement, maintain, or reestablish cybersecurity; core function of the donated technology or service must be to protect information by preventing, detecting, and responding to cyberattacks

			• Taking a neutral position with respect to protected technology, including as to the types and versions of software that can receive protection • Do not distinguish between cloud-based software and software that must be installed locally.
Alternatives Considered to cover hardware	✓		• Five, aforementioned conditions must be met, plus a 6th additional one • Alternate extra condition: Hardware can be included if a donor determines it is "reasonable and necessary" based on a risk assessment of its own organization and that of the potential recipient. • Donors would have to perform or use an existing risk assessment for its own organization AND would require the potential recipient to have a risk assessment done (donor can provide risk assessment as donated service) to determine that the donated hardware is needed to address a risk • Propose to define "risk assessment" to be based on NIST Special Publication 800-30. • They are considering additional safeguards including limiting the permitted donated hardware to certain types (multi-functional still not allowed) and requiring a donation from the recipient
Alternatives considered		✓	Alternative #1: • Safe harbor would cover specific hardware that is necessary for cybersecurity, provided that the hardware is stand-alone (not integrated within multifunctional equipment) and serves only cybersecurity purposes (i.e. two-factor authentication dongle) Alternative #2 • Safe harbor would permit entities to donate a broader range of cybersecurity technology, including hardware, provided that specified requirements are satisfied. • Proposed exception only protects items and services that meet the definition of cybersecurity technology and related services (i.e. would not cover donations of installation, improvement, or repair of infrastructure related to physical safeguards, even if they could improve cybersecurity)