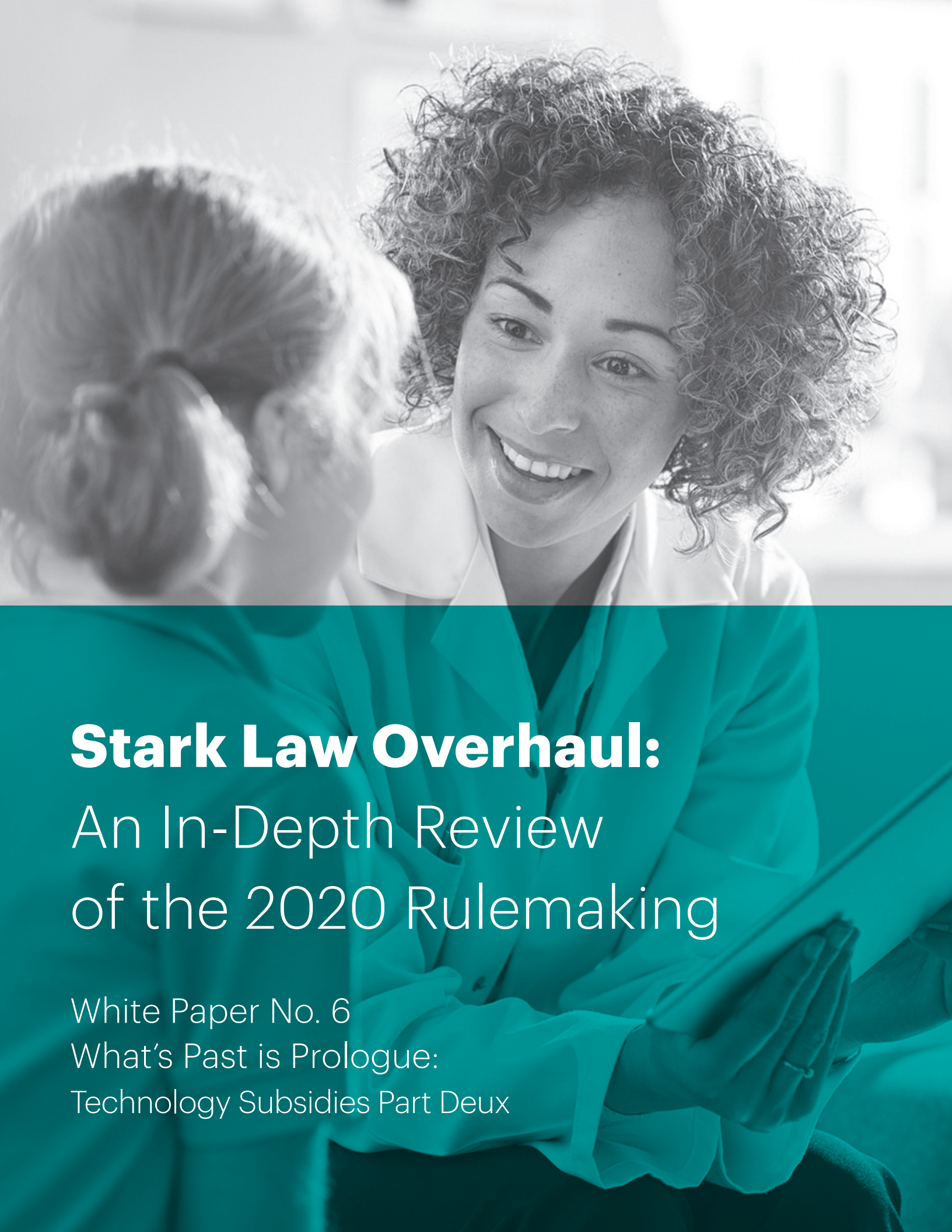

Stark Law Overhaul: An In-Depth Review of the 2020 Rulemaking

White Paper No. 6
What's Past is Prologue:
Technology Subsidies Part Deux

What's Past is Prologue: **Technology Subsidies Part Deux**

In December 2020, the Centers for Medicare & Medicaid Services (CMS) finalized its long-awaited changes to the agency's regulations governing the federal physician self-referral law, commonly known as the Stark Law (Final Rule).[1] Many of the changes had been proposed by the agency in an October 2019 proposed rulemaking (Proposed Rule).[2] The Final Rule represents the most significant Stark Law rulemaking in more than a decade. The Health Care Group at Dentons US is presenting a series of seven webinars, each with a companion white paper, addressing the principal components of the Final Rule. This is the sixth of these white papers. It addresses changes made in the Final Rule to update, clarify and expand the electronic health records exception (EHR Exception)[3] and create a new exception for donations of cybersecurity technology and services (Cybersecurity Exception).[4]

1 The Stark Law is codified at 42 U.S.C. § 1395nn, 1396b(s), and 42 C.F.R. § 411.350 *et seq.* The Final Rule was published at 85 Fed. Reg. 77492 (Dec. 2, 2020).

2 84 Fed. Reg. 55766 (Oct. 17, 2019).

3 42 C.F.R. § 411.357(w).

4 42 C.F.R. § 411.357(bb).


To learn more about the event series, please **click here**.

Contents

I. EHR Exception

A. Background

In 2006, CMS established the regulatory EHR Exception pursuant to its authority under Section 1877(b)(4) of the Social Security Act to permit certain arrangements involving donations of "interoperable electronic health records software" or "information technology and training services."[5] Between 2006 and 2021, the EHR Exception generally provided that donations of items and services in the form of software or information technology and training could be made provided the items and services were "necessary and used predominantly to create, maintain, transmit, or receive electronic health records" and a dozen additional conditions were satisfied.[6]

As discussed below, the Final Rule (i) eliminates the EHR Exception's "sunset" provisions, (ii) expands the range of items and services that may be protected under the EHR Exception, (iii) reduces the number of the EHR Exception's conditions from 12 to eight, (iv) modifies and clarifies the EHR Exception with respect to interoperability, information blocking and data lock-in, and (v) adds provisions regarding cybersecurity software and services, and replacement items and services.

B. Sunset Provisions

When CMS created the EHR Exception in 2006, the agency expected the need for it to diminish over time as EHR technology standardized across medical practices.[7] Based on this expectation, the 2006 EHR Exception originally was scheduled to "sunset" (i.e., expire) as of December 31, 2013 (Sunset Date).[8] In 2013, however, CMS concluded that the need to protect EHR donations had not diminished, and the agency extended the Sunset Date for another eight years, to December 31, 2021.[9] In the 2020 Final Rule, CMS decided to eliminate the Sunset Date altogether, noting that in light of the continued evolution of EHRs, the need for EHR donations—particularly in the form of upgrades, updates and replacements—is unlikely to subside, even in the face of the widespread adoption of EHR systems generally.[10]

C. EHR Definition

Historically, CMS defined "electronic health records" as "a repository of consumer health status information in computer processable form used for clinical diagnosis and treatment for a broad array of clinical conditions" (EHR Definition).[11] In order to update the EHR Definition, and more closely align it with the provisions of the 21st Century Cures Act (Cures Act),[12] in the Proposed Rule, CMS proposed revising the EHR Definition. Under the revised EHR Definition, "electronic health records" would mean "a repository" that includes "electronic health information," is "transmitted by or maintained

5 71 Fed. Reg. 45140 (Aug. 8, 2006). On the same date, the US Department of Health and Human Services, Office of Inspector General (HHS-OIG) promulgated a "safe harbor" for electronic health records (EHR) under the federal health care program anti-kickback statute (EHR Safe Harbor). *See* 71 Fed. Reg. 45110 (Aug. 8, 2006) (finalizing the EHR Safe Harbor at 42 C.F.R. § 1001.952(y)). In 2020, at the same time CMS updated the EHR Exception under the Stark Law, HHS-OIG updated the EHR Safe Harbor under the federal health care program anti-kickback statute. *See* 85 Fed. Reg. 77684 (Dec. 2, 2020). This White Paper does not address the EHR Safe Harbor or the recent changes made thereto.

6 42 C.F.R. § 411.357(w) (2020).

7 85 Fed. Reg. at 77613.

8 *Id.*

9 *Id.*

10 *Id.*

11 42 C.F.R. § 411.351.

12 Pub. L. 114-255, 130 Stat. 1033 (Dec. 13, 2016).

in electronic media," and "relates to the past, present, or future health or condition of an individual or the provision of health care to an individual."[13] In the Final Rule, however, CMS decided not to modify the EHR Definition after all, apparently concerned the proposed changes to the EHR *Definition* might create undesirable complexity and unwarranted substantive changes to the scope of the EHR *Exception*.[14]

D. Cybersecurity Software and Services

Historically, stakeholders have been unsure whether the EHR Exception protects donations of cybersecurity software and services. According to CMS, the answer is "yes," and in the Final Rule, the agency modified the text of the EHR Exception to make this clear.

- The introductory chapeau historically read as follows: "Nonmonetary remuneration (consisting of items and services in the form of software or information technology and training services) necessary and used predominantly to create, maintain, transmit, or receive electronic health records, if all of the following conditions are met...."[15]
- In the Proposed Rule, CMS proposed modifying this provision to read as follows: "Nonmonetary remuneration (consisting of items and services in the form of software or information technology and training services, *including certain cybersecurity software and services*) necessary and used predominantly to create, maintain, transmit, receive, or protect electronic health records, if all of the following conditions are met...."[16]
- In the Final Rule, CMS removed the "*certain*" qualifier, and now the clause at issue simply covers any "*cybersecurity software and services*," provided the other conditions of the EHR Exception are satisfied.[17]

In the Final Rule, then, CMS made it clear that an entity donating EHR software and providing training and other related services may use the EHR Exception for donations of related cybersecurity software and services that protect the EHR.[18] (With respect to donations of cybersecurity items and services that are unrelated to EHR, or that otherwise do not qualify for protection under the EHR Exception, the parties may be able to utilize the new Cybersecurity Exception, discussed below.)

E. Replacement Technology

In the Proposed and Final Rules, CMS recognized that even if a provider's *existing* EHR system meets current certification criteria and presents no risk to patients, there may be legitimate business and/or clinical reasons for *replacing* the provider's system.[19] Historically, however, a condition of the EHR Exception has been that the donor may not "not have actual knowledge of" or "act in reckless disregard or deliberate ignorance of, the fact that" the physician in question already "possesses or has obtained items or services *equivalent* to those provided by the donor" (Equivalent Items Condition).[20] Historically, the Equivalent Items Condition has been interpreted to prohibit the donation of many types of replacement EHR software and other technology, even though they can be prohibitively expensive for individual physicians or group practices to obtain.[21] In order to address this disconnect, in the Proposed Rule, CMS proposed revising the EHR Exception to make it clear that donations of "replacement" EHR items or services are permitted. Facing little pushback, CMS adopted its proposal in the Final Rule. Specifically, the EHR Exception now references "the donation of replacement items and services" in two places, and CMS removed the Equivalent Items Condition from the EHR Exception altogether.[22]

13 84 Fed. Reg. at 55824, 55840.

14 85 Fed. Reg. at 77614.

15 42 C.F.R. § 411.357(w) (2020).

16 84 Fed. Reg. at 55845.

17 85 Fed. Reg. at 77678.

18 *Id.* at 77611. According to CMS, a secure log-in or encrypted access mechanism included with an EHR system or EHR software suite, for example, would be cybersecurity features of the EHR items or services that may be protected under the existing EHR Exception. *Id.* at 77611 n.18.

19 84 Fed. Reg. at 55826; 85 Fed. Reg. at 77619.

20 42 C.F.R. § 411.357(w)(8) (2020).

21 84 Fed. Reg. at 55826.

22 85 Fed. Reg. at 77619.

The Final Rule also makes it clear, however, that replacement items and services will be treated as a new donation and, as such, must satisfy all of the requirements of the EHR Exception.[23] For example, as is the case with "the *initial* donation of items and services," before a physician receives "the donation of *replacement* items and service," the physician must pay 15 percent of the donor's cost for those items and services.[24] By treating a donation of replacement items and services as a new donation, CMS endeavors to strike a balance between making necessary replacements financially feasible for recipients and maintaining the safeguards necessary to protect the Medicare program (and Medicare beneficiaries) from fraud and abuse.

F. Interoperable: Definition and Deeming Provision

1. Definition

One condition of the EHR Exception is that the donated items and services must be "interoperable."[25] Historically, the definition of "interoperable" has been:

> able to communicate and exchange data accurately, effectively, securely, and consistently with different information technology systems, software applications, and networks, in various settings; and exchange data such that the clinical or operational purpose and meaning of the data are preserved and unaltered.[26]

In the Proposed Rule, CMS proposed modifying this definition to align it with the definition of "interoperability" in the Cures Act. Specifically, CMS proposed defining "interoperable" for Stark Law purposes to mean (i) "[a]ble to securely exchange data with and use data from other health information technology without special effort on the part of the user," (ii) "[a]llows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law," and (iii) "[d]oes not constitute information blocking as defined in section 3022 of the [Public Health Service Act]."[27]

In the Final Rule, CMS adopted the majority (but not all) of its proposed changes. First, more recent and independent authorities—most notably, the US Department of Health and Human Services' Office of the National Coordinator (ONC)—now address information blocking in earnest. In light of this, CMS decided to remove the third (information blocking) condition above from the final text of the "interoperable" definition.[28] CMS also deleted the phrase "without special effort on the part of the user" from the first condition above, explaining that this deletion would avoid misleadingly incorporating a certification requirement into the definition of "interoperable."[29]

23 *Id.*

24 *Id.* at 77616 (emphasis added).

25 42 C.F.R. § 411.357(w)(2).

26 42 C.F.R. § 411.351 (2020).

27 84 Fed. Reg. at 55825.

28 85 Fed. Reg. at 77611.

29 *Id.* at 77615.

As revised, then, the new definition of "interoperable" in the Stark Law regulations reads as follows:

> *Interoperable* means—
>
> 1. Able to securely exchange data with and use data from other health information technology; and
> 2. Allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law.

2. Deeming Provision

Historically, the EHR Exception provided for EHR software to be "deemed" interoperable—i.e., deemed to meet the definition of interoperable—"if, on the date it is provided to the physician, it has been certified by a certifying body authorized by the National Coordinator for Health Information Technology to an edition of the electronic health record certification criteria identified in the then-applicable version of 45 CFR part 170 [covering health information technology]" (Deeming Provision).[30]

In the Proposed Rule, CMS proposed replacing the phrase "has been certified" with "is certified" to clarify that the certification must be current and active as of the donation date (i.e., the parties cannot rely on prior certifications).[31] CMS also proposed removing the reference to "an edition" of the relevant regulatory certification criteria in order to align with changes recently made by the ONC to its certification program.[32]

In the Final Rule, CMS adopted these proposals, confirming that the certification must be current and active as of the time of donation, and deleting the phrase "an edition" in accordance with ONC certification program changes.[33] In response to questions about whether a certificate is the only means to establish that EHR is "interoperable," CMS made it clear that the answer is "no." The EHR Exception merely requires that the EHR at issue *be* interoperable at the time it is provided to the recipient; it does not prescribe the *method* for determining interoperability.[34] Simply put, while parties may take advantage of the Deeming Provision, they are not required to do so in order to establish that the EHR at issue is "interoperable."

30 42 C.F.R. § 411.357(w)(2) (2020).

31 84 Fed. Reg. at 55823.

32 *Id.*

33 85 Fed. Reg. at 77609.

34 *Id.* at 77609-10.

G. Information Blocking

Historically—and separate and apart from the definition of "interoperable" (discussed above)—the EHR Exception itself prohibited donors from "taking action to limit the use, compatibility, or interoperability of the donated items or services with other electronic prescribing or electronic health records systems,"[35] a practice now referred to as "information blocking" under the Cures Act.[36] The prohibition originally was included in the EHR Exception to promote the free exchange of data and prevent the misuse of the EHR Exception to "lock in" or "steer" patient referrals.[37]

In the Proposed Rule, CMS proposed updating the information blocking prohibition to align it more closely with the terminology used in more recent federal legislation and guidance.[38] In the Final Rule, however, CMS—consistent with its decision regarding the definition of "interoperable"—decided to remove the information blocking prohibition from the EHR Exception altogether. Once again, the agency noted that other federal departments were both better equipped to regulate information blocking and had already begun to do so.[39]

H. Recipient Cost Sharing Requirement

Finally, to address the program integrity risks inherent in unlimited donations of EHR items and services, the EHR Exception historically has included a cost-sharing requirement; specifically, the EHR Exception required that "[b]efore receipt of the items and services, the physician pays 15 percent of the donor's cost for the items and services" (Cost-Sharing Requirement).[40] In the Proposed Rule, CMS responded to complaints that the Cost-Sharing Requirement has been overly burdensome and a barrier to adoption of EHR by proposing two alternatives.

- Under the first alternative, CMS would eliminate or reduce the amount small or rural physician organizations would be required to contribute. With respect to this alternative, CMS solicited comments on how to define "small or rural physician organization" and "rural physician organization."[41]
- Under the second alternative, CMS would eliminate the Cost-Sharing Requirement altogether. With respect to this alternative, CMS solicited comments on the potential impact it might have on (i) the use and adoption of EHR technology and (ii) Medicare program integrity.[42]

Finally, CMS indicated that regardless of whether it retained the Cost-Sharing Requirement for some or all physician recipients, it would consider modifying or eliminating the Cost-Sharing Requirement with respect to *updates* relating to previously donated EHR software.[43]

In the Final Rule, however, CMS went in a third direction. The agency retained (i) the Cost-Sharing Requirement for initial donations and donations of replacement items and services, and (ii) the requirement that physicians pay their 15 percent cost share in advance of the receipt of the donated items and services.[44] With respect to "updates," however—including updates to initial or replacement items—the Final Rule permits the recipient to pay its cost contribution amount "at reasonable intervals,"[45] which CMS leaves undefined. Lastly, the Final Rule continues to prohibit the donor (or any person related to the donor) from financing the physician's cost-sharing obligations, but the agency also notes that these obligations may be funded by the physician's practice group/organization on the physician's behalf.[46]

35 42 C.F.R. § 411.357(w)(3) (2020).

36 Pub. L. 114-255, § 3022, 130 Stat. 1033, 1176-77.

37 84 Fed. Reg. at 55823.

38 *Id.*

39 85 Fed. Reg. at 77611.

40 42 C.F.R. § 411.357(w)(4) (2020).

41 84 Fed. Reg. at 55825.

42 *Id.*

43 *Id.*

44 85 Fed. Reg. at 77616.

45 *Id.*

46 *Id.* at 77616, 77618.

II. Cybersecurity Exception

A. Background

Prior to 2021, there was no Stark Law exception for donations of cybersecurity technology and related services. In response to numerous comments and suggestions, however, CMS proposed the adoption of such an exception in 2019, and the Final Rule adopted that proposal.[47] The new Cybersecurity Exception is codified at 42 C.F.R. § 411.357(bb).

When it proposed the new exception, CMS stated that it would "help improve the cybersecurity posture of the health care industry by removing a perceived barrier to donations" designed "to address the growing threat of cyberattacks that infiltrate data systems and corrupt or prevent access to health records and other information essential to the delivery of health care."[48] The agency noted that while the risks of cyberattacks often reside at certain "weak links," they ultimately are borne by every component of the health care ecosystem, imposing high costs on the health care industry, causing disclosures of protected health information, and endangering patients.[49] Indeed, CMS expected that donors and recipients often would be part of the same integrated system—such as a hospital and a physician using a shared interface—and, as a result, donors would be providing technology and related services in an effort to protect both the recipients and *themselves* (i.e., the *donors*) from cyberattacks.[50]

In developing the Cybersecurity Exception, CMS attempted to strike a balance between the government's policy aims (e.g., the rapid adoption of effective cybersecurity measures) and the risks of Medicare program abuse (which can arise when DHS Entities are permitted to provide expensive items and services to referral sources). Thus, while the Cybersecurity Exception, as finalized, is quite broad in terms of the scope of protected cybersecurity technology and related services, it is limited by a host of conditions, including the requirement that the cybersecurity technology and related services be "necessary and used predominantly to implement, maintain, or reestablish cybersecurity."

B. Proposed Rule

In the Proposed Rule, CMS proposed new regulatory definitions for both "cybersecurity" and "technology."[51] Both definitions were intended to be as broad as possible in order to promote the adoption of cybersecurity measures.[52] The proposed definition of "cybersecurity" was drawn from the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure,[53] but CMS requested comment on whether this definition was sufficiently tailored to the health care industry.[54] The proposed definition of "technology" was "any software or other types of information technology *other than hardware*."[55]

47 84 Fed. Reg. at 55830.

48 *Id.*

49 *Id.*

50 *Id.* at 55831.

51 84 Fed. Reg. at 55831.

52 *Id.*

53 *Id.*

54 *Id.*

55 *Id.* (emphasis added).

CMS proposed excluding donations of hardware on the grounds that hardware often is expensive and can be used for purposes other than cybersecurity. Under these circumstances, CMS feared that permitting donations of hardware would increase the risk that the donations were "being made to influence referrals."[56] CMS solicited comments, however, on two alternative approaches: (i) permitting the donation of hardware that *exclusively* serves cybersecurity purposes; and (ii) permitting the donation of hardware if it was determined to be necessary as a direct result of donor- and recipient-specific cybersecurity risk assessments.[57]

Aside from these two definitions, the proposed Cybersecurity Exception included four requirements.

- First, the Cybersecurity Exception would apply only to technology and services that are "necessary and used predominantly to implement, maintain, or reestablish cybersecurity."[58]
- Second, the donation of technology or services could not be determined in a manner that "takes into account the volume or value of referrals or other business generated between the parties."[59]
- Third, neither the physician nor the physician's practice could make the donations of technology or services "a condition of doing business with the donor."[60]
- Fourth, the arrangement had to be "documented in writing."[61]

CMS requested comment on several aspects of these requirements, including whether the agency should:

- create a "deeming" provision that parties could use to establish that certain arrangements would be deemed "necessary and used predominantly" to implement, maintain, or reestablish cybersecurity (e.g., by conforming to a widely-recognized cybersecurity framework);
- create a "deeming" provision consisting of a list of recipient selection criteria that, if met, would result in the arrangement being deemed not to take into account the volume or value of referrals or other business generated by the physician (similar to an analogous provision in the EHR Exception);
- restrict the types of entities that could be donors;
- require a minimum contribution from the recipient to the cost of the donation; and/or
- specify the terms required for a writing documenting the donation arrangement.[62]

C. Final Rule

The Final Rule adopted the Cybersecurity Exception as proposed, with only one substantive modification.[63] Specifically, CMS removed "other than hardware" from the definition of "technology," noting that the lines between hardware, software, services and other technology have been "increasingly blurred" and that multiple components are frequently "packaged together as a bundle."[64] CMS clarified, however, that the definition of "technology" was specific to the Cybersecurity Exception and not intended to affect the meaning of (i) "information technology" used in other regulations or (ii) "technology" appearing in the EHR Exception.[65] Further, although CMS did not adopt either of its proposed alternatives to a hardware ban, the agency emphasized that "parties remain free, and are encouraged, to perform risk assessments to determine donor and recipient vulnerability to cyberattacks and to assist in creating their own cybersecurity programs."[66]

CMS decided not to establish any "deeming" provisions in the Cybersecurity Exception. According to the agency, the level of specificity that would be required for the provisions to be triggered could result in confusion, and the provisions could be interpreted as prescriptive requirements that would prevent parties

56 *Id.*

57 *Id.* at 55831-32, 55834-35.

58 *Id.* at 55832.

59 *Id.* at 55833.

60 *Id.* at 55833, 55847.

61 *Id.* at 55834.

62 *Id.* at 55832-34.

63 85 Fed. Reg. at 77631.

64 *Id.* at 77638.

65 *Id.* at 77637.

66 *Id.* at 77639.

from making beneficial cybersecurity improvements. This would be particularly true, CMS noted, where (as here) the health care industry is faced with a "new exception that applies to emerging and rapidly evolving arrangements."[67]

CMS rejected several proposed changes to the definition of "cybersecurity," including those that would have (i) expressly included all data analytics and reporting functionality, (ii) covered processes such as "identifying" or "recovering" from cyberattacks, and (iii) limited the definition to only "effective" cybersecurity or cybersecurity measures designed to protect a particular subject.[68] CMS also:

- rejected the concerns raised by certain commenters that the Cybersecurity Exception could (i) have anti-competitive effects or limit physician autonomy, because large health care entities could offer larger donations, or (ii) result in inappropriate information blocking;[69]

- declined to adopt alternatives to the "necessary and predominantly" terminology used in the exception, such as requiring the technology or services to have a "clear nexus" to cybersecurity or to "substantially further the interests of strengthening technology;"[70] and
- declined to establish specific requirements for documenting the donation arrangement, acknowledging, however, that documentation in the form of a signed agreement would be a "best practice."[71]

In its entirety, then, the Cybersecurity Exception as promulgated in the Final Rule is remarkably concise, straightforward and broad, reading (in its entirety) as follows:

> (bb) Cybersecurity technology and related services.
>
> (1) Nonmonetary remuneration (consisting of technology and services) necessary and used predominantly to implement, maintain, or reestablish cybersecurity, if all of the following conditions are met:
>
> i. Neither the eligibility of a physician for the technology or services, nor the amount or nature of the technology or services, is determined in any manner that directly takes into account the volume or value of referrals or other business generated between the parties.
>
> ii. Neither the physician nor the physician's practice (including employees and staff members) makes the receipt of technology or services, or the amount or nature of the technology or services, a condition of doing business with the donor.
>
> iii. The arrangement is documented in writing.
>
> (2) For purposes of this paragraph (bb), "technology" means any software or other types of information technology.

67 *Id.* at 77641.

68 *Id.* at 77636, 77638.

69 *Id.* at 77632.

70 *Id.* at 77634.

71 *Id.* at 77643.

III. Conclusion

Although the clarifications of, and modifications to, the EHR Exception in the Final Rule were relatively modest, the establishment, terms and conditions of the Cybersecurity Exception are noteworthy. Industry stakeholders clearly are concerned about the rising costs of cybersecurity technology and related services, the vulnerability of the entire health care system caused by any weak link in the chain, and the enormous costs and patient risk associated with cyberattacks. CMS responded to these concerns by crafting a Cybersecurity Exception that covers a broad range of technology and services and is specifically designed to "improve the cybersecurity posture" of the health care industry. While the Cybersecurity Exception does require that the technology or service be "necessary and used predominantly" for cybersecurity purposes, CMS declined a host of proposed alternatives that would have narrowed the scope of the defined terms or further restricted the applicability of the Cybersecurity Exception. In addition, by adopting broad terminology and definitions, and aiming for consistency with the popular NIST cybersecurity framework, the Cybersecurity Exception should cover technology and services that are both "currently available, as well as technologies and services that will be developed in the future."[72]

72 *Id.* at 77635.

Stark Law Overhaul Series: An In-Depth Review of CMS's Final Rule

REGISTER HERE

On December 2, 2020, CMS published a final rule incorporating long-awaited changes to the agency's regulations governing the federal physician self-referral law, commonly known as the Stark Law. The final rule represents the most significant Stark Law rulemaking in more than a decade.

Dentons' analysis of this major regulatory overhaul will be presented in a series of seven webinars, each with a companion white paper, addressing all of the principal components of the 2020 rulemaking. Each webinar will provide an in-depth review of a related group of provisions, offer practical examples of the new rule in operation, and highlight questions and issues that remain unresolved.

Join us Thursdays from 12:30-1:45 pm ET for our bi-weekly **Stark Law Overhaul webinar***

Date	Time	Topic*
March 18	12:30-1:45 pm ET	Rolling Up Our Sleeves: A Stark Law Refresher and Clearing the Brush
April 1	12:30-1:45 pm ET	Separating the Wheat From the Chaff: Providing Greater Flexibility for Technical and Low-Dollar Violations
April 15	12:30-1:45 pm ET	Key Standards (Part I): Distinguishing and Defining the 'Volume or Value' Requirement
April 29	12:30-1:45 pm ET	Key Standards (Part II): 'Fair Market Value' and 'Commercial Reasonableness' Standards, and Indirect Compensation Arrangements
May 13	12:30-1:45 pm ET	New Wine in Old Bottles: Providing Greater Flexibility Under Existing Exceptions
May 27	12:30-1:45 pm ET	What's Past is Prologue: Technology Subsidies Part Deux
June 10	12:30-1:45 pm ET	The Problem of the Square Peg and the Round Hole: When FFS and Managed Care Collide

** CLE credit is being applied for in Arizona, California, Georgia, Illinois, Missouri, New Jersey, New York, Texas and Virginia. Credit for all other states must be applied for and submitted by individual attendees. Compliance with each state's MCLE requirements is the sole responsibility of the attendee.*

Health Care

Dentons has more than 50 health care lawyers and professionals in the US. Our group closely collaborates with Dentons' corporate, litigation, tax, government enforcement and white collar investigations, public policy and other prominent practice groups, making Dentons the firm of choice among a wide range of health care entities both within the US and worldwide, including health care providers, suppliers, insurers, and network managers.

Key Contacts

The Dentons lawyers presenting this series, including Gadi Weinreich, Chris Janney and Ramy Fayed, are widely recognized as Stark Law thought leaders. They and other members of Dentons' US Health Care practice group have assisted countless clients in navigating this unforgiving law since its enactment in 1989, lectured extensively on its challenges and pitfalls, and authored multiple articles as well as two editions of *The Stark Law: A User's Guide to Achieving Compliance*.

Chris Janney
Partner

Ramy Fayed
Partner

Esperance Becton
Associate

ABOUT DENTONS

Dentons is the world's largest law firm, connecting talent to the world's challenges and opportunities in more than 75 countries. Dentons' legal and business solutions benefit from deep roots in our communities and award-winning advancements in client service, including Nextlaw, Dentons' innovation and strategic advisory services. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and world-class talent challenge the status quo to advance client and community interests in the New Dynamic.

dentons.com

CSBrand-59672-Stark-Law-Series-White-Paper-6-03 — 26/05/2021