August 24, 2018

Seema Verma
Administrator
Centers for Medicare & Medicaid Services
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Administrator Verma:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to comment on the Centers for Medicare and Medicaid Services' (CMS) proposed rule, "Medicare Program; Request for Information Regarding the Physician Self-Referral Law," published in the *Federal Register* on June 25th.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With more than 2,700 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate the effective use of information management to improve the health and healthcare in the communities they serve.

We appreciate the Administration's efforts to reduce regulatory burdens on healthcare providers. When the physician self-referral law – frequently referred to as the Stark law - was enacted in 1989, it was implemented with the intent of separating the profit motive from care delivery. The healthcare delivery system today, however, is a vastly different landscape than in was then. When discussing the Regulatory Sprint to Coordinated Care initiative, you stated, "While Stark is an important anti-fraud protection for Medicare, it was enacted in 1989 and has been interpreted and reinterpreted, and is out dated. It has become a significant barrier to innovative arrangements that drive value." We agree.

Our members are responsible for the digitization of healthcare, something that is fundamental to spurring a healthcare system that is driven by value rather than volume. They have identified several barriers erected by the Stark rules which inhibit the move to value and have suggestions for improving the regulatory climate. Our top recommendations for achieving this are outlined below followed by more detailed comments:

1. **Electronic Health Record (EHR) exception:**
    a. The donation exemption for interoperable technology and training which is slated to sunset by 2021 should be extended;
    b. This exception should also be expanded to permit donations that improve data exchange (i.e. population health, interfaces) that will improve providers' ability to move to value-based arrangements, as well as, care coordination in more traditional fee for service models of care; and
    c. CMS should examine how burdens for meeting Stark can be reduced for providers already participating in Accountable Care Organizations (ACOs), Clinically Integrated Networks (CINs), and Organized Health Care Arrangements (OHCAs).
2. **Creating a cybersecurity exception:** To help improve the cybersecurity posture of providers and better protect patient information, as well as improve patient safety, an exception should be granted for the donation of cybersecurity technology and services.

Administrative Complexity

The administrative costs in our healthcare system have been well-chronicled and contribute greatly the cost of delivery, yet little in the way of value or improved outcomes. For instance, according to Change Healthcare (now McKesson,)[1] 9% of hospital claims representing $262 billion out of $3 trillion are denied annually and appeals cost $118 per claim or $8.6 billion annually. Adding to this is the regulatory complexity around a myriad of rules – often competing ones – which providers must navigate when information can be shared, under what conditions and with whom, which amounts to what one of our members likened to "multilayered quilts or multiple layers of federal requirements laying on top of one another." This complexity is so prolific that our members are left to create complicated internal matrixes to help them try and discern under what conditions patient information may be shared.

So much of the healthcare dollar is gobbled up by collecting the correct documentation and then the headache and time involved with submitting, resubmitting, prior authorizations and appeals that place a huge toll on the overall system. Complicating matters is codes are used to determine and calculate the risk adjustment factor for a patient, which is then used to determine the total cost of care for a patient in a year. Together these present tremendous burdens for providers in navigating the revenue cycle and coding requirements. Our members try to work with individual practices who

[1] http://healthyhospital.changehealthcare.com/change_healthcare_analysis_262_billion_in_healthcare_claims_initially_denied_in_2016/

do not have enough support staff to navigate these hurdles, or who must expend resources on these tasks that otherwise could be used to invest in the services and technology needed to support robust health information exchange. We appreciate CMS' willingness to consider new Stark exceptions that can reduce some of the burdens confronting our members in today's healthcare system.

Extending and Expanding the EHR Donation Exception

Expansion to Support Data Exchange Costs

Through Stark exceptions, providers such as hospitals are permitted to make donations of software or information technology and training services used predominantly to create, maintain, transmit, or receive EHRs and the EHRs must be interoperable. Hardware, however, is not allowed to be donated under this exception. Providers (i.e., hospitals) may make permissible donations (up to 85% of the costs) to other providers (i.e., independent clinicians). The exceptions governing this Stark exemption were extended to December 31, 2021 in a final rule published in 2013. While there has been a substantial growth in hospital-employed physicians, there are still many independent practices with whom our members do business and who continue to benefit from the ability to receive a donated EHR.

Several of our members have taken advantage of this exception to donate EHRs and many feel the EHR donation exception has been pivotal in spurring adoption among smaller providers. They believe that the exception is still warranted but they also feel it should be expanded. It is widely recognized that a properly interconnected healthcare system, where data flow freely to authorized parties (and patients) in a uniform manner and is integrated seamlessly into the clinical workflow, is needed. Better data exchange is also needed to manage risk, which is heavily dependent on information sharing around clinician performance, administration and clinical information. The expectation is data exchange can help foster better outcomes and lower costs and thus is critical to moving the nation toward a healthcare system that is rooted in value rather than volume. Therefore, regulatory flexibility that allows expanding the Stark EHR donation exemption could help facilitate better data exchange, help providers better managed risk and help interoperability flourish.

Today, it is no longer enough to just reimburse for the cost of an EHR; financial support is needed to support data exchange. The myriad interfaces clinicians needed to facilitate data exchange are frequently cost prohibitive and these costs are growing as more providers establish digital connections.

Unfortunately, even with the move to application programming interfaces (APIs), providers will still face the need to pay for interfaces that will introduce a whole new wave of costs in addition to those needed to connect disparate EHRs. The costs to support this interconnectedness are growing as the policy and clinical expectations around data sharing grow. The use of medical devices connected to EHRs is growing; the use of mobile applications is exploding, especially as

consumer become more engaged in their care; and technology is fostering remote care and the ability of patients to share patient-generated data. Further, as providers grapple with the opioid epidemic that has swept the nation, the need to access Prescription Drug Monitoring Programs (PDMPs) also requires costly interfaces.

Contributing further to these issues is that some providers are further along their data exchange journey. While the Health Information Technology for Economic and Clinical Health (HITECH) Act incentives were aimed at hospitals and clinicians and spurred substantial uptake of EHRs among these providers, there is a need to exchange data across the care continuum such as long-term, post-acute and behavioral health providers. Some of these providers are further behind in their ability to exchange data and establishing interfaces for these providers can be a costly endeavor. Additionally, providers who may have more advanced data exchange capabilities still need to connect with these providers to thrive in risk-based and traditional fee-for-service models of care to control costs, coordinate care, and of course, improve patient outcomes.

Further, by our estimations, using the voluntary Trusted Exchange Framework, once finalized by the Office of the National Coordinator for Health Information Technology (ONC), will not be without costs. It remains unclear where the funding the Qualified Health Information Networks (QHINs) (i.e. health information exchanges) will come from, but we do not expect this to be free. The Recognized Coordinating Entity (RCE) could pass costs off to the QHINs who could then pass them off to the providers. While the costs for providers participating in CommonWell and Carequality are absorbed today by the vendors, it is conceivable that at some point they will be passed onto providers.

Finally, national standards for data reconciliation are burdensome to clinicians as they become overwhelmed by vast amounts of patient data that should be reviewed, but they may not be able to easily reconcile it in the manner software engineers envisioned. This problem will grow until artificial intelligence is able to catch up and help extract key unique data from the vast data presented. Therefore, expanding the EHR Stark donation to support more data exchange would be extremely helpful.

Taken together, the task of connecting our healthcare system is a daunting one from a cost standpoint and a Stark exemption that further supports data exchange across the care continuum would be highly beneficial. Providers, especially small practitioners, need support with health information exchange (HIE) connections, establishing Direct Addresses, reporting to various registries, PDMP connections, and importantly population health – costs which can far exceed the cost of a donated EHR.

Expansion to Support ACOs, CINS, and OHCAs

Many of our members are engaged with ACOs and CINs; as such, their revenue can be at-risk. Working with small, independent practices is pivotal in these arrangements and the ability for them to be able to exchange data can make the difference between success and failure. Unfortunately, small practitioners struggle not only with the costs to exchange information, but the prohibitive

costs of interfaces can prevent them from participating in an ACOs or CINs. Our members are precluded under current rules from donating the cost for "their side" of the interface. As one member reflected on these challenges, "We can't continue to layer financial burden on small practices – they can't fall back on a big organization. They (small practices) won't participate in Shared Savings if they had to pay. They are ALL at risk if they fail or don't participate."

Since participation in ACOs, contracts aimed at helping providers coordinate care; CINs, contracts that allow providers to meet a common set of quality, cost and safety measures; and OHCAs, contracts which allow for sharing of protected health information (PHI); we encourage CMS to examine what providers are already required to meet in these arrangements which could be waived under Stark rules to leverage more efficiencies and reduce the regulatory burden.

Care Coordination Needs to Support Fee-for-Service

While new contracts aimed at managing costs and improving value through risk contracts are growing, our members also need of ways to sign network type arrangements that show provider alignment in coordinating care and addressing complex outcomes goals even when they are not in traditional shared risk arrangements. Ultimately, many providers are independently held to such standards through their payor arrangements (i.e. quality goals) and these can only be achieved with collaboration, coordination and data sharing. Data sharing arrangements, however, remain complex because of lack of industry-wide data loss risk mitigation. The result is providers require a rigorous process for evaluation of a partner's data center, security standards, and contract language. This includes currently requiring any entity have Soc 2 Type 2 certification for their data center and DR site.

Moreover, integrating data also remains expensive and time-consuming for providers even if they are not in risk-based models. This investment will not be made with organizations directly unless they are aligned around common outcomes goals, whether contractually or not. Stark exceptions are thus critical if providers want to see investments made that improve the health of their communities.

Cybersecurity

As we have raised with CMS previously, the issue of cybersecurity is paramount to providers and they take their responsibility to protect and safeguard patient information very seriously. However, as the healthcare system has become more digitized in recent years, the CMS policies which mandate data exchange have increased, and the use of mobile applications and connected medical devices are proliferating, the ability of providers to keep up with the ever-growing number of cybersecurity threats is often outpaced. We worry their ability to fend-off sophisticated attacks could harm patient safety. Therefore, it is critical that policymakers identify as many incentives as possible to help providers safeguard patient data.

In fact, the Cybersecurity Industry Task Force Report[2] mandated by the Cybersecurity Act of 2015 includes an entire section within their report (page 35) that discusses the myriad of issues associated with the anti-kickback and Stark statutes. The report says:

> *A regulatory exception to the Stark Law and a safe harbor to the Anti-Kickback Statute to protect certain donations of electronic health records (EHR) effectively addresses management of technology between health care entities and serves as a perfect template for an analogous cybersecurity provision. Physician groups confront a myriad of financial challenges. Often these financial constraints limit their ability to manage the EHR software without trained security professionals who have the expertise to provide sufficient cybersecurity programs to protect their patient records. We need to empower small providers or suppliers (e.g., physician practices) to actively manage their security posture, not hinder them. Often organizations want to provide technology to ensure smaller business partners do not become a liability in the supply chain. An exception may provide for this assistance without creating fear of violating the Stark Law or Anti-Kickback Statute.*

One way CMS can do this – among others – is to create a Stark exception that would allow providers to donate cybersecurity technology (both hardware and software), training and tools to other providers (i.e. under-resourced or less sophisticated ones) to improve the overall cybersecurity posture of our industry. As one member of ours reflected, "the sum of the parts is only as strong as the weakest link."

Several of our members struggle to help those independent practices with which they are engaged with under risk or other contracts, upon whom they already donate EHR software. The reality today is that clinically integrated networks simply cannot afford to ignore the cybersecurity posture of smaller, independent practices. Yet, the inability to donate these types of services makes it even harder for them to coordinate care.

As CMS considers these issues, we believe it is important to note that the agency's own data indicate that one of the primary reasons that providers have incurred a penalty under the Meaningful Use / Promoting Interoperability program is rooted in a failed risk assessment. And, with the agency moving to scoring system that offers zero points for either hospitals or clinicians, there is no financial incentive offered to help providers better their cybersecurity posture, yet they will be financially penalized if they do not meet the requirement.

Conclusion

CHIME appreciates that CMS is looking to identity and remove regulatory barriers that increase the complexity of healthcare delivery and impede the move to value, care coordination and data exchange. We welcome the opportunity to comment on this important issue. Should you have any

[2] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

questions concerning our comments, please contact Mari Savickis, vice president, federal affairs, at mari.savickis@chimecentral.org.

Sincerely,

Russell Branzell, FCHIME, CHCIO
President & CEO, CHIME

Cletis Earle
Chair, CHIME Board of Trustees
Vice President and CIO
Kaleida Health