December 31, 2019

The Honorable Seema Verma
Administrator
Centers for Medicare & Medicaid Services
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Acting Inspector General Chiedi
Office of the Inspector General
U.S. Department of Health and Human Services
Cohen Building
330 Independence Avenue, SW
Washington, DC 20201

Re: **OIG-0936-AA10-P***: Medicare and State Healthcare Programs: Fraud and Abuse; Revisions To Safe Harbors Under the Anti-Kickback Statute, and Civil Monetary Penalty Rules Regarding Beneficiary Inducements*

CMS-1720-P: *Medicare Program; Modernizing and Clarifying the Physician Self-Referral Regulations*

Dear Administrator Verma and Acting Inspector General Chiedi:

The American Telemedicine Association (ATA), is pleased to comment on the companion proposed rules issued on October 17, 2019: (1) *Medicare and State Healthcare Programs: Fraud and Abuse; Revisions To Safe Harbors Under the Anti-Kickback Statute, and Civil Monetary Penalty Rules Regarding Beneficiary Inducements (OIG-0936-AA10-P)*; and (2) *Medicare Program; Modernizing and Clarifying the Physician Self-Referral Regulations (CMS-1720-P)*.

As the only organization completely focused on advancing telehealth, the ATA is committed to ensuring that everyone has access to safe, affordable and appropriate care when and where they need it, enabling the system to do more good for more people. The ATA represents a broad and inclusive member network of technology solution providers and payers, as well as partner organizations and alliances, working to advance industry adoption of telehealth, promote responsible policy, advocate for government and market normalization, and provide education and resources to help integrate virtual care into emerging value-based delivery models.

Our members are dedicated to improving health through technology-enabled health and care management and delivery systems and ATA appreciates your dedication to removing barriers to

providing value-based care. Below we offer comments on the proposed rules and how they may align with ATA's guiding principles:

- Eliminate artificial government barriers to telehealth, including geographic discrimination and restrictions on the use of telehealth in managed care.
- Prevent new barriers to telehealth, such as clinical practice rules that impose higher standards for telehealth-provided services than in-person care.
- Encourage the use of telehealth to reduce health delivery problems, such as provider shortages.
- Promote payment and service delivery models to increase consumer and payer value using telehealth.
- Enhance consumer choice, outcomes, convenience, and satisfaction.

Value-Based Exceptions/Safe Harbors

One significant area of promise which has received bipartisan support in Congress is increasing Medicare coverage and reimbursement for services delivered via telemedicine. CMS has also proactively expanded payment for remote physiologic monitoring (RPM) and new communication technology-based services. However, as the reimbursement landscape shifts and adoption of digital technologies increases, HHS's fraud, waste, and abuse rules must be updated to reflect the new manner in which care is provided.

In order to effectively implement telemedicine in diverse settings, employed providers should be able to receive the equipment from the employer (such as a hospital). Similarly, providers should be able to provide patients with technology that enables high-value care, such as devices for remote patient monitoring. Finally, providers should be empowered to provide telehealth technology to targets groups of patients with a particular condition or stage of condition.

ATA applauds the expansion of Stark and Anti-Kickback Statute (AKS) exceptions/safe harbors to ease burdens for providers engaged in value-based payments. We also support the safe harbors excluding care coordination and value-based arrangements from renumeration. These safe harbors will help facilitate appropriate telehealth technology for both upstream and downstream providers. However, we urge HHS to expand the proposed waivers for non-risk baring arrangements. The requirements for the Care Coordination Arrangements safe harbor are more onerous than for the proposed risk-bearing safe harbors. In recognition of the data that shows

that value-based arrangements take on more risk with experience and over time, the requirements should be aligned across the waivers.

As proposed, the new value-based exceptions each have their own administrative and compliance requirements, which places unnecessary burden on providers and is antithetical to providing efficient, high-quality care. The ATA supports uniform requirements for all value-based arrangements, regardless of the level of provider risk and believes that a requirement of a methodology written in advance provides sufficient protection against gaming. Such consistency would also resolve the apparent misalignment between AKS and Stark requirements for similar arrangements (e.g., whether writing is required and what it must contain).

Finally, in order for providers to make use of – and comply with – the new safe harbors and exceptions, HHS should clearly define all of the terms it uses in the regulations (for instance, describing whether "evidence-based, valid outcome measure" is an objective or subjective standard).

Patient Engagement and Support Safe Harbor

We support proposals to create a new safe harbor "for certain tools and supports furnished under patient engagement and support arrangements to improve quality, health outcomes, and efficiency" (1001.952(hh)). This language should make it clear that value-based care arrangements and research arrangements may allow for telemedicine, RPM, and other digital tools and services to be provided at no cost without being considered a beneficiary inducement or triggering a violation of the AKS.

We also support OIG providing the waiver or offset of cost-sharing obligations for care management and RPM value-based use cases.

Statutory Exception for Telehealth Technologies for In-home Dialysis

The ATA fully supports the proposal to amend the beneficiary inducements CMP definition of "remuneration" related to in-home dialysis services. Allowing end-stage renal disease (ESRD) patients who receive home dialysis to obtain monthly ESRD-related clinical evaluations via telehealth technologies, will remove barriers to care for many patients. We also agree with the proposal to require that any such technologies come from the provider or facility that is then-providing services like home dialysis, telehealth visits, or other ESRD care to the patient.

With respect to other safeguards HHS is considering, we believe that providers and dialysis facilities should be allowed to provide telehealth technology to certain groups of patients who meet certain criteria. A requirement to provide the technology to all patients would wasteful and

limit providers' ability to put technology in the hands of the patients who would most benefit from it.

Cybersecurity Technology

Small and Under-resourced Providers
The ATA applauds efforts to better support small and under-resourced providers and ease the ability for these organizations to invest in technology and services to protect infrastructure and safeguard patient data. As health care becomes increasingly interconnected, policies to support providers become more critical. As you know, cybersecurity vulnerabilities can spread quickly, and health care providers are now faced with managing cybersecurity risks that challenge even the best resourced organizations. From a cybersecurity perspective, the health care system is only as strong as its weakest links. Patients and providers of all sizes benefit when small and under-resourced providers can better protect themselves.

Patching
Providers have an obligation to ensure patient safety. Patching and updates are widely accepted as being critical to guarding against cybersecurity threats and the U.S. Department of Health & Human Services (HHS) and its work alongside industry as part of the CISA 405(d) Task Group call out the lack of patching as a significant vulnerability for most health care organizations and recommend it as a best practice. It is important to note that the technology (or accompanying security updates/fixes) would not be a one-time donation but something that would need to be maintained over time in the case of hardware and software.

Both CMS and OIG have proposed that patching and updates will not be an allowable donation that would receive protection under the exception/safe harbor. This could create significant complications in disaggregating when technology is permitted to be donated. Often, patching is given to providers for free as it is built into the contracts with vendors. We request clarification on whether accepting routine or critical updates would implicate a violation of the exception/safe harbor. Some patches also may be aimed at security while others may be more general. Has there been consideration on permitting patching when it is needed for security purposes?

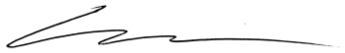
Definition of Technology
Both CMS and OIG have called for excluding hardware from the permitted type of technology which is protected under the cybersecurity donation exception/safe harbor. This approach could impede the success of this exception/safe harbor. First, the lines between what is considered hardware vs software is increasingly being blurred. Also, by breaking out hardware from the definition of technology it does not account for the pace of innovation. Second, vendors do not typically break out the cost of hardware vs software – the price or value is based upon the totality of the device. An example would be a networking device that is running software. Precluding the

donation of hardware, therefore, could create barriers to addressing increased risk of cyber attacks, which ultimately puts patients at greater risk.

Liability
Cybersecurity presents healthcare providers with additional challenges when managing liability and related legal risks. We recommend clarifying whether donor providers and donating entities could incur liability if the recipient of donated technology experiences a cyber incident. For example, if a donating entity provides a risk assessment under the exception/safe harbor and the provider suffers a breach due to a cyberattack, what liability would the donor incur? If not addressed, the cybersecurity technology donation exception / safe harbor may be underutilized and fail to benefit the broader health care system as envisioned by CMS and OIG.

Thank you for the opportunity to provide feedback and your efforts to modernize the regulations on these critical issues that are essential to the success of the regulatory sprint to coordinated care**.** If you have any questions or would like to further discuss our comments, please contact me at kharper@americantelemed.org.

Sincerely,



Kevin Harper
Director, Public Policy