



JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

ama-assn.org
t (312) 464-5000

October 25, 2018

Daniel R. Levinson
Inspector General
Office of Inspector General
U.S. Department of Health and Human Services
Attention: OIG-0803-N
Cohen Building, Room 5541C
330 Independence Avenue, SW
Washington, DC 20201

Dear Inspector General Levinson:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to provide our views on how the anti-kickback statute and the civil monetary penalties (CMP) law impose undue burdens on physicians and serve as obstacles to coordinated care and efforts to deliver better value and care for patients. We commend the U.S. Department of Health and Human Services (HHS) and the Office of Inspector General (OIG) for focusing on removing unnecessary government obstacles to coordinated care, real or perceived, caused by the anti-kickback statute and CMPs. In updating the statute, OIG should allow physicians to receive reimbursement for the value of care provided, and promote competition and choice by allowing physicians the same opportunities hospitals have in delivering care.

Significant changes in health care payment and delivery have occurred since the enactment of the anti-kickback statute. Numerous initiatives are attempting to align payment and coordinate care to improve the quality and value of care delivered. The delivery of care is going through a digital transformation with innovative technology. However, the anti-kickback statute—in its over 40 years of existence—has not commensurably changed.

The anti-kickback statute and CMP law were enacted in a fee-for-service world that paid for services on a piecemeal basis. The policy reasoning behind the fraud and abuse laws is to act as a deterrent against overutilization, inappropriate patient steering, and compromised medical judgment with heavy civil and criminal penalties, such as treble damages, exclusion from participation in federal health care programs, and potential jail time.

The health care system is moving to a world that pays health professionals to manage episodes of patient care in a more comprehensive and coordinated way. However, this approach to payment can run afoul of the fraud and abuse laws. For example, even if the primary purpose of an arrangement is to improve patients' health outcomes, as long as one purpose of the arrangement's payments is to induce future referrals, the fraud and abuse laws are implicated (e.g., an arrangement that pays for a nurse coordinator

to coordinate a recently discharged patient's care among a hospital, physician specialists, and a primary care physician may induce future referrals to the primary care physician to avoid an unnecessary readmission to the hospital).

Fostering the shift to Alternative Payment Models (APMs) has necessitated reviewing and, in some situations, updating fraud and abuse laws to ensure that they do not unduly impede the development of value-based payment. Through specific statutory authority, both the Centers for Medicare & Medicaid Services (CMS) and OIG have deemed it necessary to waive the requirements of certain fraud and abuse laws to test the viability of innovative models that reward value and outcomes.

Outside of those models, however, the fraud and abuse laws may still pose barriers to initiatives that align payment with quality and improve care coordination. Tying compensation to the value of care provided, equipping providers with tools to improve care, and investing in tools to clinically and financially integrate all may run afoul of these laws. For example, in certain circumstances the anti-kickback statute impedes care coordination by prohibiting physicians from coordinating care on behalf of their patients. This leaves the patient, in addition to dealing with the physical and emotional aspects of a disease or condition, to coordinate their own care in a fragmented and siloed system. Placing the obligation on the patient to know how to properly manage follow-up care without the assistance of their physician or care coordinator may have a negative impact on patient care and the physician-patient relationship.

Accordingly, the AMA has urged Congress and the Administration to **create an anti-kickback statute regulatory safe harbor to facilitate coordinated care and promote well-designed APMs**. This safe harbor should be broad, covering both the development and operation of a model to allow physicians to transition to an APM model, and provide adequate protection for the entire care delivery process to include downstream care partners, entities, and manufacturers who are linking outcomes and value to the services or products provided. Moreover, as OIG examines updating the anti-kickback statute regulations to reflect the transition from volume to value base care, we urge OIG to consider modernizing these regulations to address other realities of the health care delivery system, including the advent and growth of pharmacy benefit managers, expansion of delivery outside the four walls of a traditional health care setting, increase risk of cyber attacks, and development and increase use of digital health tools.

I. Promoting Care Coordination and Value-Based Care

a. Potential Arrangements

Generally, the AMA has concerns about the ability of financial arrangements to satisfy anti-kickback safe harbors that involve shared savings or incentive payments being distributed based on the value of care provided by physicians either in a group or independent practice. For example, a financial arrangement that is based on managing patients with a chronic disease rewards an individual physician for properly coordinating care with nursing staff and intervening proactively with a patient to prevent unnecessary hospitalization. This reward can be interpreted as running afoul of the anti-kickback statute as remuneration in return for referring an individual for an item or service that is payable under a federal health care program (i.e., referral for a follow-up primary care visit in lieu of an unnecessary hospitalization).

The AMA is also concerned about potential anti-kickback statute liability for arrangements and activities that fall within the exceptions from the definition of remuneration under the CMP law. Specifically, the exception from the beneficiary inducement CMP for remuneration that promotes access to care and poses

a low risk of harm could implicate anti-kickback statute liability. For example, beneficiaries being provided a dedicated mobile treatment plan app that allows for daily engagement with the physician and ensures greater compliance with agreed to evidence-based treatment plans so that early intervention can be taken to avoid unnecessary hospitalizations and emergency room visits fits within the exception from remuneration because it helps beneficiaries access care by improved future care-planning by their physician. However, the arrangement is still subject to anti-kickback statute liability.

b. Additional or Modified Safe Harbors

i. *APM Safe Harbor*

The AMA believes that a single exception—if broad enough—provides sufficient protection for all types of financial arrangements (e.g., shared savings, bundled payments, incentive payments). The AMA has no objections in amending existing exceptions or definitions to promote care coordination. However, a multifaceted approach that establishes multiple new exceptions would only add more burden and complexity to an already confusing law.

As above, **OIG should create an anti-kickback statute regulatory safe harbor to facilitate coordinated care and promote well-designed APMs.** The financial arrangement that fits within the exception should be for the purposes of operating and developing an APM. Protecting the development of the APM is a key reform that could help incentivize physicians to transition from the Merit-based Incentive Payment System (MIPS) to APMs. The development should cover start-up and infrastructure costs. The exception should cover any arrangement between the APM, one or more of the APM's participants, downstream care partners, entities, and manufacturers who are linking outcomes and value to the services or products provided, or a combination thereof.

Flexibility is important for innovation. Yet flexibility in a new payment system also may raise fraud and abuse concerns. To help address these concerns, the safe harbor could incorporate provisions that increase transparency and accountability; require the arrangement to be tied to the goals of the alternative payment model; and allow freedom of choice for patients by prohibiting stinting on medically necessary care. While participation agreements work well in the context of specific payment models, the AMA believes they would likely be impractical for the federal health care programs generally. As an alternative, the parties to the arrangement could set forth in writing the arrangement; the goals for patient care quality, outcomes, utilization, or costs; and the items and services covered under the arrangement.

ii. *Personal Services and Management Contracts Safe Harbor*

For value-based arrangements, the AMA urges OIG to modify the personal services and management contracts safe harbor to eliminate the requirements that aggregate compensation be set in advance, be consistent with fair market value, and not be determined in a manner that takes into the account the volume or value of any referrals. Instead, with value-based arrangements, **OIG should allow personal services and management contracts that reward value and allow for incentive payments for efficient and better care.**

“Set in advance” is not defined. OIG interprets the requirement to mean that the total aggregate compensation to be paid over the term of the contract must be determined at the outset of the arrangement. Thus, per hour, use, or click compensation will generally not qualify for safe harbor protection. In addition, shared savings calculations or incentives based on value are generally not set in

advance because the shared savings are not calculated until after the fact. Originally, the set in advance requirement was created to prevent a kickback that could occur if an otherwise legitimate payment were adjusted periodically to reward a party for referring patients and overutilization. These concerns do not exist in value-based care. In coordinating care under a value-based arrangement, improper referrals and overutilization can result in repayment or in receiving no incentives or shared savings.

iii. Warranty Safe Harbor

The AMA urges that the warranty safe harbor be expanded to include bundled items. Currently, the warranties safe harbor protects remuneration consisting of “any payment or exchange of anything of value under a warranty provided by a manufacturer or supplier of an item to the buyer . . . of the item.”¹ Thus, a bundle of items is not covered by the safe harbor. Given that bundled payments are a type of APM, OIG should expand the warranty safe harbor for these types of bundled arrangements.

The risk of fraud and abuse is low when the items or services provided subject to a warranty are paid through one bundled payment for all the items and services the health care provider furnishes in connection with a rendered service (e.g., hospital stay, surgery). Generally, the warranty attached to the provision of the items is against an undesirable result, such as readmission after surgery. This type of warranty benefits both the patient and the federal health care programs. Furthermore, to prevent inappropriate steering the OIG could add a provision that such warranty is not exclusive and not subject to any quota or minimum purchase.

iv. Electronic Health Records Safe Harbor

Physician-led team-based care needs electronic access across different care sites to information necessary to properly coordinate care and to make appropriate and informed decisions about patient care. Accordingly, OIG should revise the electronic health records (EHR) safe harbor to promote coordination and interoperability by: (1) making the exception permanent; (2) broadening the definition of “electronic health record” beyond clinical diagnosis and treatment to include activities like information sharing and data analysis; and (3) allowing for the donation of technology that replaces similar technology.

v. Clarification in Guidance

The AMA believes the following opportunities exist where OIG could clarify its position through guidance, such as a law enforcement policy statement, as opposed to regulation.

As previously mentioned, the AMA is concerned about potential anti-kickback statute liability for arrangements and activities that fall within the exceptions from the definition of remuneration under the CMP law. Thus, **OIG should issue a law enforcement policy statement that meeting the requirements of the promoting access to care exception from the definition of remuneration from the beneficiary inducement CMP poses a sufficiently low risk of fraud and abuse under the anti-kickback statute.** Furthermore, OIG will use its enforcement discretion and not pursue anti-kickback cases when the items or services meet the promoting access to care exception from the definition of remuneration from the beneficiary inducement CMP.

¹ 42 CFR § 1001.952(d).

This policy statement should be issued because the exception from remuneration already includes the concept of posing a low risk of harm to patients and the federal health care programs, OIG has already placed the burden of demonstrating low risk of harm under the CMP onto health care providers,² and using the Advisory Opinion process for a case-by-case determination for every instance of a beneficiary incentive is an impracticable solution. Moreover, these incentives help deliver higher quality, better coordinated care; enhance value; and improve the overall health of patients and should not be subject to the anti-kickback statute when posing a low risk of harm to patients.

Please see Section III of this response to the request for information regarding a potential policy statement regarding the waiver of nominal cost-sharing amounts.

vi. Impact of Safe Harbors on Competition and Administrative Burden

The AMA strongly supports and encourages competition between and among health care providers, facilities, and insurers as a means of promoting the delivery of high quality, cost-effective health care. Providing patients with more choices for health care services and coverage stimulates innovation and incentivizes improved care, lower costs, and expanded access. The health care system in the United States is undergoing substantial consolidation through mechanisms ranging from mergers and acquisitions to institutional affiliations to single service agreements. Such consolidation reduces choices for patients without controlling costs. This is unacceptable—in the Executive Order *Promoting Health Care Choice and Competition*, President Trump made clear the Administration’s commitment to advancing competition in health care markets.

When considering revising or creating new safe harbors or CMP exceptions from remuneration, OIG should ensure that any change is entity agnostic and does not further promote consolidation of the health care system. This means that a rural, one physician practice should have the same capability to implement the exception as a large health system. Safe harbors that favor certain larger entities or increase burden may lead to further consolidation and increase costs. Physicians should not have to be employed by a hospital or sell their practice to a hospital to participate in Medicare or in innovative delivery models. Moreover, any change should not unnecessarily increase administrative burden on practices. The mounting burdens of the modern health care delivery system are taking a toll on physicians by contributing to the growing problem of work-induced burnout and emotional fatigue. Ultimately, physicians should be able to maintain their independent practice while at the same time have access to the infrastructure and resources necessary to participate in APMs.

c. Definitions of Critical Terminology

The term “alternative payment model” should be broadly defined to cover a variety of financial arrangements that promote value-based care and care coordination (e.g., advanced alternative payment models, physician-focused payment models, MIPS APMs, and other payer APMs). The term should also provide flexibility to cover future financial arrangements that are not yet created or contemplated. Thus, any definition of the term “alternative payment model” should include a provision that allows the Secretary to designate any other arrangement as an APM through public notice.

² See 81 Fed. Reg. 88368, 88391 (Dec. 7, 2016).

The term “care coordination” should provide protection for interactions between all individuals and entities involved in physician-led team-based care. Patient care in the community can involve physicians creating a care plan and working with allied health professionals like nurses, care coordinators, social workers, and home health aides to implement the care plan.

II. Beneficiary Incentives

a. Types of Incentives

The AMA recommends that OIG allow for in-kind remuneration as a beneficiary incentive for wellness and managing chronic diseases (e.g., adherence to treatment plans and management programs that promote the health and wellness of beneficiaries). Rewarding adherence can help the patient understand the importance of the interaction between lifestyle, disease, and prescribed treatment. Ultimately, these programs are worthwhile because they could substantially reduce the cost of health care over time.

b. Incentives Contributing to Better Care

Promoting patient adherence to treatment regimens and chronic disease management programs improves quality of care, care coordination, and patient engagement by promoting community and individual awareness of health risks and resources, reduce cost by eliminating unnecessary care, engage at-risk populations, and provide valuable beneficiary education.

c. Potential Restrictions to Reduce the Risk of Fraud and Abuse

The AMA understands that the beneficiary inducement CMP is intended to prevent overutilization, improperly influencing patient treatment decisions, skewing patient selection, and creating a competitive disadvantage for providers who cannot afford providing incentives. However, incentives can also increase access, reduce inefficiencies, improve coordination of care, and enhance patient health. Thus, certain restrictions or safeguards may be needed to allow proper beneficiary incentives while preventing incentives that negatively impact professional independence. Potential safeguards could include:

- Establishing a reasonable connection between the items and services and the health and wellbeing of a beneficiary;
- Limiting the items or services to in-kind incentives;
- Requiring that the items or services relate to improving public health and safety (e.g., preventative care, vaccines) advancing adherence to a care plan, or helping manage chronic disease(s) or condition(s);
- Prohibiting any public promotion or advertisement of the incentive; or
- Barring eligibility for an incentive that results in the withholding of appropriate medical services or in the denial of patient access to such services.

d. Medication Adherence and Medication Management

The AMA fully supports beneficiary incentives for medication adherence and medication management. Poor medication adherence represents a significant source of wasteful health care spending. While the causes are complex and systemic, beneficiary incentives may help solve part of this approximately \$290

billion problem.³ That said, beneficiary incentives connected to medication adherence and medication management should not be treated differently than other types of beneficiary incentives. OIG should allow for beneficiary incentives for all types of adherence and management programs that promote the health and wellness of beneficiaries.

e. Required Disclosures to Beneficiaries Regarding Incentives

The AMA supports physician disclosure of their financial interest in the facility, product, or equipment to patients; informing patients of available alternatives for referral; and assuring patients that their ongoing care is not conditioned on acceptance of the recommended referral.⁴ Additionally, any disclosure should not unnecessarily increase the administrative burden on physicians or take time away from rendering care.

III. Cost-Sharing Obligations

Cost-sharing obligations are particularly problematic when the costs associated with reasonable collection efforts exceeds the cost-sharing amount that would be potentially collected. Thus, similar to the OIG Policy Statement regarding gifts of nominal value, OIG should also **issue guidance allowing for the waiver of cost-sharing amounts when the cost-sharing amount is nominal**. For example, through the physician fee schedule, CMS is proposing to expand Medicare coverage to include services like virtual care visits. CMS proposes to pay approximately \$15 for a virtual check-in service.⁵ With a 20 percent cost sharing amount, a beneficiary would pay approximately \$3. As defined by CMS and OIG, the costs of any “reasonable collection effort” would far exceed the \$3 collected.⁶ Requiring such efforts creates waste, adds unnecessary administrative burdens, and inappropriately increases costs to physician practices. Thus, OIG should issue a Policy Statement allowing for the waiver of nominal cost-sharing amounts. Alternatively, OIG should amend its interpretation of “reasonable collection efforts” under section 1128A(i)(6)(A)(iii)(II) of the Social Security Act so that these collection efforts do not include situations where the costs of the collection efforts by the provider exceeds the cost-sharing amount that would be potentially collected.

Additionally, cost-sharing obligations are particularly problematic with chronic care management (CCM) services. Patients may be discouraged from taking advantage of this high-value service due to the cost-sharing amounts. **OIG should create a safe harbor to waive cost-sharing amounts for CCM and other high-value services** that may save money through better care coordination, improved patient outcomes, and avoiding unnecessary hospitalizations. This safe harbor could be tied to APMs that are focused on managing chronic conditions where the cost-sharing amount may discourage a patient from

³ New England Healthcare Institute, *Improving Patient Medication Adherence*(2011), available at https://www.nehi.net/bendthecurve/sup/documents/Medication_Adherence_Brief.pdf.

⁴ AMA, *Physicians’ Self Referral*, Policy H-140.861 (2015); AMA, Code of Medical Ethics, *Opinion 9.6.9 Physician Self Referral* (2017).

⁵ 83 Fed. Reg. 35704, 35723 & 35786 (July 27, 2018).

⁶ OIG has stated that “reasonable collection efforts” are those efforts that a reasonable provider would undertake to collect amounts owed for items and services provided to patients. 65 Fed. Reg. 24400, 24404 (Apr. 26, 2000). In 2016, OIG cited the CMS Provider Reimbursement Manual’s description of reasonable collection efforts including requiring “providers to issue a bill for the patient’s financial obligation” and “other actions such as subsequent billings, collection letters, and telephone calls or personal contacts with this party which constitute a genuine, rather than a token, collection effort.”⁸¹ Fed. Reg. 88368, 88374 (Dec. 7, 2016) (citing CMS, Provider Reimbursement Manual, CMS Pub. 15-1, § 310).

seeking primary care. Removing this unnecessary impediment to the physician-patient relationship could return impressive results. Regular appointments allow providers to more closely monitor patients and identify complications before they require hospitalization and to establish a more regular, wellness-based relationship between physician and patient. This can encourage the patient to reach out to a physician before resorting to more costly options such as calling an ambulance.

IV. Cybersecurity-Related Items and Services

The AMA is deeply concerned that our nation's health care providers have been insufficiently prepared to help meet the cybersecurity challenges of an increasingly digital health care system. We firmly believe that this is a national priority and that physicians and other health care providers need tools to secure sensitive patient information in the digital sphere. Unfortunately, the anti-kickback statute prevents the sharing of cybersecurity tools and resources, thereby hindering collaborative industry cybersecurity efforts. Thus, **the AMA recommends that OIG create a safe harbor that allows for the sharing of cybersecurity items and services.**

a. Need for Safe Harbor

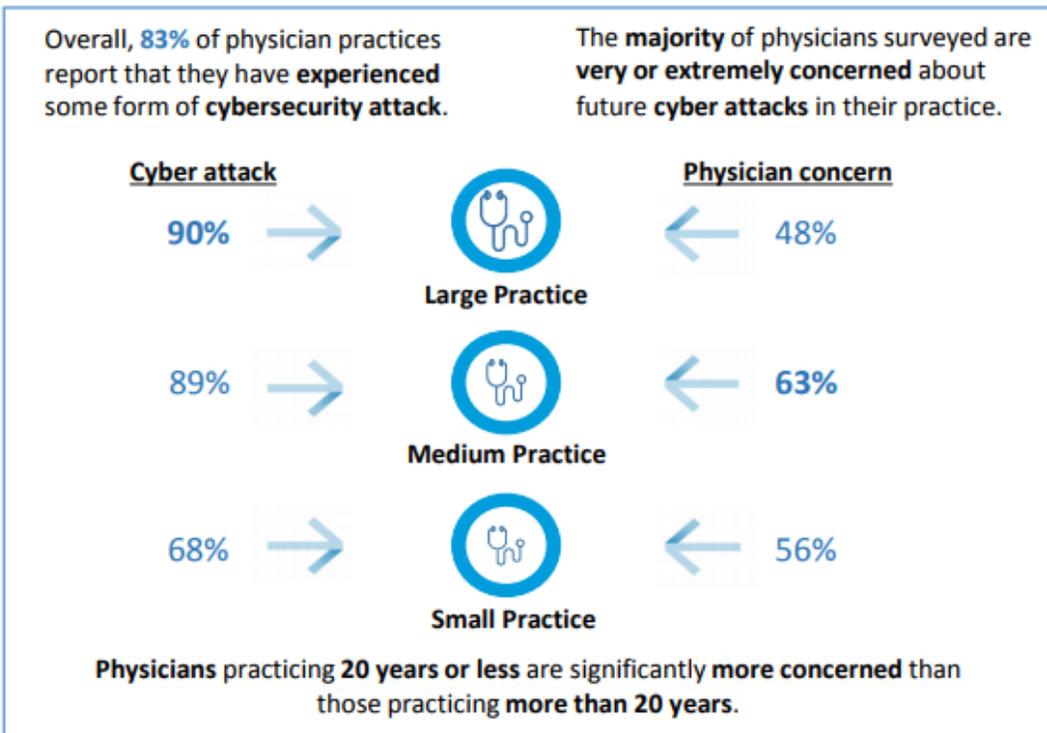
A cybersecurity safe harbor is needed because: (1) cybersecurity is a patient safety issue; (2) cyber attacks are inevitable; (3) physicians need tools and resources to prepare for cyber attacks; and (4) the health care sector exchanges health information electronically more than ever before, putting the entire health care ecosystem at risk.

Cybersecurity is a patient safety issue. The AMA, along with Accenture, recently completed a cybersecurity survey of 1,300 physicians.⁷ The top three cybersecurity concerns that physicians identified were interruption to EHR access, EHR security (including compromised patient data), and general patient safety concerns. The health care community must recognize that cybersecurity is not only a technical issue, but also a patient safety issue. OIG also recognizes that HHS “must protect its beneficiaries by fostering a culture of cybersecurity among its partners and stakeholders.”⁸ Thus, the federal government should create positive incentives—like a cybersecurity safe harbor—to promote the adoption of good cyber hygiene without creating additional physician burden.

Cyber attacks are inevitable and physicians are concerned about future attacks. As shown in the figure below, physicians recognize that it is not “if” but “when” they will experience a cyber attack.

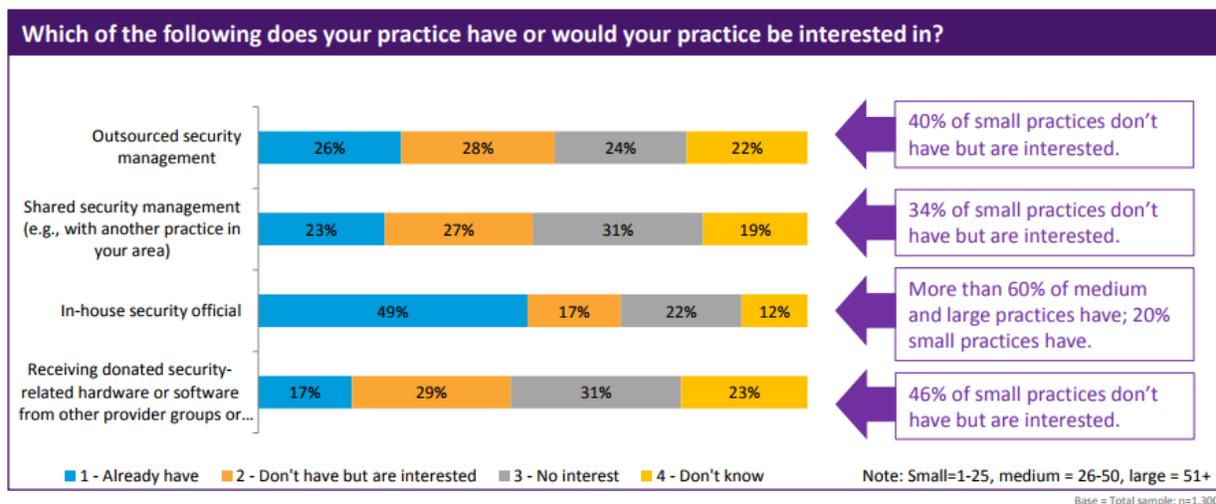
⁷ AMA, *Medical Cybersecurity: A Patient Safety Issue*, (Dec. 2017), available at <https://www.ama-assn.org/about/medical-cybersecurity-patient-safety-issue>.

⁸ OIG, Top Management #10: Protecting HHS Data, Systems, and Beneficiaries from Cybersecurity Threats (2017), available at <https://oig.hhs.gov/reports-and-publications/top-challenges/2017/2017-tmc.pdf#page=45>.



These attacks can jeopardize patient safety and interrupt physician practice operations. Most physician practices experience up to four hours of downtime because of a cyber attack, but some take almost a full day to resume operations.

Physicians are interested in receiving tools and resources to increase their cyber hygiene:



Physician practices spend a substantial amount on cybersecurity. For example, in our qualitative review, a nine-physician practice spent \$250,000 per year and a 50+ physician regional medical center spent \$440,000 per year. We further note that only one in five small physician practices have an in-house

security official. Thus, small practices need extra help in navigating cybersecurity challenges to help them prepare for cyber attacks and ensure patient data remains confidential and does not land in the hands of criminals. The federal government needs to empower physicians to actively manage their security posture, not hinder them.

Finally, cybersecurity affects the entire health care ecosystem. Technology has increased connectivity and collaboration in all facets of the health care delivery system. Indeed, the AMA's cybersecurity survey shows that 85 percent of physicians believe it is "very" or "extremely" important to share data to provide efficient, quality care but are concerned about how to share it securely. This integration is increasingly important as the industry moves towards value-based care and provides more care outside the four walls of a brick-and-mortar health care practice.

Unfortunately, adversaries now have more potential entry points to exploit than ever before and more data to access when they do. These adversaries will target the weakest link in the chain, which may be a physician office. Many physicians will be adopting new EHR technologies in the coming months. These EHRs include de novo data exchange functionality, i.e., application programming interfaces (API), which can serve as new attack surfaces and vectors—exposing a physician's information network to additional threats.⁹ Even if the physician office houses relatively few health care records, it may be connected to other health systems with significantly more data. Accountable Care Organizations and other value-based models may overlook potential opportunities to work with small community physicians if those practices cannot afford proper cybersecurity tools. Put simply, small practices may be priced out of participation in APMs if they cannot access affordable cybersecurity tools. Allowing hospitals and other large providers to share and donate cybersecurity support to physicians will help ensure the security of patient information and improve care coordination among the ecosystem.

OIG recognizes that cybersecurity threats are a top management challenge to HHS and identifies fostering a culture of cybersecurity beyond HHS as a key component of protecting beneficiaries.¹⁰ Moreover, OIG recently formed a multidisciplinary Cybersecurity Team comprised of auditors, evaluators, investigators, and attorneys focused on combatting cybersecurity threats within HHS and the health care industry. Furthermore, OIG calls on HHS to use policy levers to encourage cybersecurity efforts without creating undue burden. The AMA believes that OIG should use its own policy lever by issuing a safe harbor to promote cybersecurity throughout the health care system.

b. Structure of Safe Harbor

Overall, the AMA stresses that any cybersecurity safe harbor be easy to understand, interpret, and enforce so that donors and recipients can readily distinguish permissible activities from those that violate the anti-kickback statute. We believe that the current EHR safe harbor may act as template for a new cybersecurity safe harbor. We also note that HHS' recent Health Care Industry Cybersecurity Task Force report to Congress recommended exploring potential impacts to the anti-kickback statute, the Physician

⁹ WEDI Workgroup for Electronic Data Interchange, *The Rampant Growth of Cybercrime in Healthcare* (February 2017), available at <https://www.wedi.org/docs/publications/cybercrime-issue-brief.pdf?sfvrsn=0>

¹⁰ HHS OIG, *Top Management and Performance Challenges Facing HHS, Challenge #10: Protecting HHS Data, Systems, and Beneficiaries From Cybersecurity Threats* (2017), available at <https://oig.hhs.gov/reports-and-publications/top-challenges/2017/2017-tmc.pdf#page=45>.

Self-Referral Law, and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners.¹¹

c. The Types of Persons That Would Be Parties to, or Benefit From, Such Arrangements

Donors: The AMA supports a broad scope of protected donors to significantly further the important public policy goal of promoting cybersecurity. Donors of cybersecurity should be an individual or entity that provides patients with health care items or services covered by a federal health care program and submits claims or request for payment for those items or services (directly or pursuant to reassignment) to Medicare, Medicaid, or other federal health care programs. Donors should also be health plans as defined 42 C.F.R. 1001.952(1)(2), EHR vendors, and ancillary service providers because they can play a central role in the adoption and use of cybersecurity. Furthermore, while the AMA understands that OIG enforcement experience raises questions about unscrupulous manufacturers, OIG should consider manufacturers as potential donors because they can play a direct and central patient care role that justifies safe harbor protection for the provision of cybersecurity items and services and in protecting the security of devices in the health care ecosystem.

Recipients: Recipients of donated cybersecurity items and services should be practitioners, providers, and suppliers that furnish service directly to federal health care program beneficiaries and those that furnish services to health plan enrollees. This would include physicians, group practices, physician assistants, nurse practitioners, nurses, therapists, audiologists, pharmacists, nursing facilities, federally qualified health centers (FQHCs), and others.

d. The Particular Types of Items That Would Be Involved

The AMA believes that non-monetary remuneration should be covered to include items in the form of hardware and software. This includes upgrades of equipment and software to enhance functionality; license, right to use, and intellectual property. The scope of covered items and services would also include hardware network appliances because many cybersecurity software products require the use of a specific hardware device to operate. Software could include malware prevention, endpoint security, data protection/encryption, continuous monitoring, log management, and traffic filtering products.

e. The Types of Services That Would Be Involved

The AMA believes that non-monetary remuneration should be covered to include services in the form of training or security education, testing services, management and monitoring services, and on-demand help desk/repair/maintenance services. Cybersecurity education and training are key. The Health Care Industry Cybersecurity Task Force Report highlights that cybersecurity must be governed with a collaborative approach to protect patients and specifically notes as one of its six high-level imperatives the need to “increase health care industry readiness through improved cybersecurity awareness and education.”¹² Meeting this goal requires an educated workforce to make evidence-based decisions that are reliant on secure data. The AMA’s cybersecurity survey further reflects this need for education. Many physicians surveyed reported wanting more educational support, including a simplified summary and checklist of

¹¹ Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care Industry* (June 2017), available at <https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf>.

¹² *Id.*

HIPAA guidelines, accessible tips for good cyber hygiene, and a how-to guide for assessing cybersecurity risks.

Additionally, physicians desire shared cybersecurity management (e.g., three physician practices pool resources together to pay for a third party to act as a security official to manage each practice's cybersecurity efforts). While this may fall under the personal services and management contracts safe harbor, the AMA is concerned about any perceived potential referral patterns between the physician groups and would ask that this type of arrangement be explicitly included in a cybersecurity safe harbor.

f. Other Considerations in Developing a Cybersecurity Safe Harbor

Definitions: In defining cybersecurity, OIG should look to other government agencies. For example, the AMA recommends using the National Institute of Standards and Technology (NIST) definition of cybersecurity which includes the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."¹³

Value of Technology: The EHR safe harbor has a 15 percent contribution that must be incurred by the recipient of the EHR technology. The AMA would not object to a similar approach with a cybersecurity safe harbor. However, OIG should consider whether it is appropriate for small or rural practices to receive such tools for free, have a lower percentage contribution, or have a free amount up to a specific dollar amount and then have a percentage contribution. Furthermore, the AMA believes that anything above a 15 percent contribution level would impose a prohibitive financial burden on physicians.

g. Mitigating Potential Risks or Unintended Consequences

The AMA understands that OIG has a long-standing concern about the provision of free or reduced price goods or services to an existing or potential referral source. Thus, an appropriate balance must be struck between promoting the adoption of cybersecurity across the health care ecosystem and the underlying purpose of the anti-kickback statute to promote the professional independence of physicians receiving this support and the donors providing it.

OIG may want to consider requiring that the recipient conduct a security risk analysis, a risk assessment, or have a cybersecurity framework implemented to receive donated cybersecurity items/services. The AMA stresses that this approach should be flexible to allow for multiple avenues of compliance, not be overly burdensome, and to take into account a practice's size and resources.

To guard against overutilization, increased federal program costs, corruption of medical decision making, and unfair competition, OIG could consider the following protections:

- Not making the receipt of cybersecurity tools or services a condition of doing business with a donor;
- Not restricting the use of cybersecurity tools or services for any patient regardless of payor;

¹³ NIST, *Glossary of Terms from the Computer Security Resource Center*, available at <https://csrc.nist.gov/Glossary/?term=3817#AlphaIndexDiv> (definition of "cybersecurity").

- Creating a written agreement that is signed by the parties that identifies with specificity about the tools or services provided or shared; and
- Assurance that eligibility to receive donated cybersecurity tools or services, including the amount or nature of the technology, could not be determined in any manner to take into account the volume or value of referrals or other business generated between the parties.

h. How Such Items or Services Reduce Cybersecurity Risks

Cybersecurity items and services reduce risks by preventing threats from occurring, identifying and tracking threats, analyzing and translating threat data into actionable information, and providing the ability to act on that information.

i. Risks if HHS Takes No Action

Substantial risk to patient safety exists if HHS takes no action. The OIG itself identifies fostering a culture of cybersecurity beyond HHS as a key component of protecting beneficiaries.¹⁴ Moreover, OIG recognizes that many public and private individuals, organizations, and agencies operate aging equipment and outdated software, which can create challenges in terms of keeping up with technological advances and evolving cybersecurity threats.

The health care system cannot deliver effective and safe care without deeper digital connectivity. If the health care system is connected, but insecure, this connectivity could subject patients to unnecessary harms and risks.¹⁵ A lack of necessary tools and resources diminishes the ability to respond to internal and external threats. Furthermore, as stated above, small practices may be priced out of participation in APMs if they cannot access affordable cybersecurity tools

The risks to patient safety are expected to increase as health care becomes more dependent upon the Internet of Things, including non-regulated devices that may affect privacy, safety, and patient care. These may include such diverse products as manufacturing systems, building control systems, and wearable devices. In addition, precision medicine (which customizes treatment based on a patient's environment, lifestyle, and genes) is likely to provide great benefits to patient care while also generating potential risks as information is shared.¹⁶

The AMA appreciates your consideration of a cybersecurity safe harbor. OIG, along with CMS and other interested HHS stakeholders, should consider scheduling an open-door forum to discuss the risks and benefits of donating cybersecurity technology.

¹⁴ HHS OIG, *Top Management and Performance Challenges Facing HHS, Challenge #10: Protecting HHS Data, Systems, and Beneficiaries From Cybersecurity Threats* (2017), available at <https://oig.hhs.gov/reports-and-publications/top-challenges/2017/2017-tmc.pdf#page=45>.

¹⁵ Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care Industry* (June 2017), available at <https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf>.

¹⁶ *Id.*

V. Telehealth under Section 50302(c) of the Bipartisan Budget Act of 2018

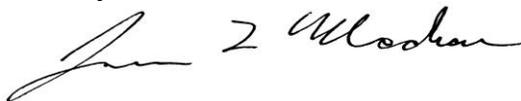
The AMA recommends that OIG define “telehealth technologies” to match the technologies that address services on the Medicare Part B telehealth list. Medicare telehealth services are limited by statute and regulation to two-way audio-visual, real time communication between a patient and a physician or other qualified health professional. CMS notes that section 1834(m) of the Social Security Act applies only to a discrete set of physicians’ services that ordinarily involve, and are defined, coded, and paid for as if they were furnished during an in-person encounter between a patient and a health care professional. A consistent statutory definition of telehealth does not exist among various federal agencies. The telehealth definition is even varied within the Social Security Act. However, for the Medicare Part B program, which includes end-stage renal disease (ESRD), the statutory definition remains unchanged and encompasses a limited modality. Thus, for purposes of defining “telehealth technologies” under section 50302(c), OIG should adopt the technologies that address the services under the current Part B definition of telehealth so that all Part B telehealth services—ESRD or otherwise—are treated consistently and in the same manner.

VI. Conclusion

As initiatives advance to align payment and care coordination to improve the quality and value of care delivered, physician leadership is instrumental to optimizing care, improving population health, and reducing costs. Physicians provide the care, take care of the patients, and see the cost inefficiencies and overutilization. In helping physicians achieve the goals of value-based care, we urge OIG to create an anti-kickback statute regulatory safe harbor to facilitate coordinated care and promote well-designed alternative payment models.

Thank you for the opportunity to comment. The AMA is committed to engaging with OIG and other stakeholders going forward on ensuring that legal structures keep pace with evolving health care delivery and payment systems. We offer our assistance as OIG considers the impact of the anti-kickback statute on physician participation in innovative payment and delivery models. Should you have any questions, please contact Paul Westfall, Washington Counsel, Division of Legislative Counsel at paul.westfall@ama-assn.org or 202-789-7430.

Sincerely,

A handwritten signature in black ink, appearing to read "James L. Madara". The signature is fluid and cursive, with a large initial "J" and "M".

James L. Madara, MD