



JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

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

February 26, 2018

Daniel R. Levinson
Inspector General
Office of Inspector General
U.S. Department of Health and Human Services
Attention: OIG-127-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 the U.S. Department of Health and Human Services (HHS) Office of Inspector General (OIG) with our recommendations in response to the annual Solicitation of new Safe Harbors and Special Fraud Alerts (OIG-127-N). The following outlines additional safe harbor provisions that we believe will promote innovation and allow physicians to modernize our nation's health care system.

Innovative Payment and Delivery Models

The fraud and abuse laws—including the Anti-Kickback Statute—can stand in the way of payment and delivery system innovation. Fostering improvements in the delivery of care has necessitated reviewing and, in some situations, relaxing fraud and abuse laws to ensure that they do not impede the development of alternative payment models that link payments to quality, efficiency, and patient health outcomes. 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.

The AMA is supportive of the fraud and abuse waivers and recommends the continuance of these waivers in current and future models. However, the waivers apply to a limited number of entities. Tying compensation to the quality, outcomes, and spending on care; equipping providers with tools to improve care; and investing in tools to clinically and financially integrate all may run afoul of these laws. More options and flexibility are needed to encourage physician-led alternative payment arrangements on a wider scale. Thus, broader flexibility from the fraud and abuse laws is needed to help realize the full potential of innovative models.

The AMA urges OIG to create a safe harbor to facilitate coordinated care and promote well-designed alternative payment models. This safe harbor should be broad, cover both the development and operation of a model, and provide adequate protection for the entire care delivery process to include downstream entities and manufacturers who are linking outcomes and value to the services or products provided.

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 have provisions from the fraud and abuse waivers:

- Increased transparency and accountability through board approval;
- Requiring the arrangement to be tied to the goals of the alternative payment model; and
- Allowing freedom of choice for patients and prohibiting stinting on medically necessary care.

While participation agreements work well in the context of specific payments models, the AMA believes they would likely be impractical for Medicare generally. As an alternative, the parties to the arrangement could set forth in writing the arrangement, their goals for patient care quality, utilization, and costs, and the items and services covered under the arrangement.

The AMA asks that OIG set forth a clear and commonsense safe harbor concerning the formation of innovative delivery models so that physicians can pursue integration options that are not hospital driven. Physicians should not have to be employed by a hospital or sell their practice to a hospital in order to participate in innovative delivery models. 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 alternative payment models.

Cybersecurity Safe Harbor

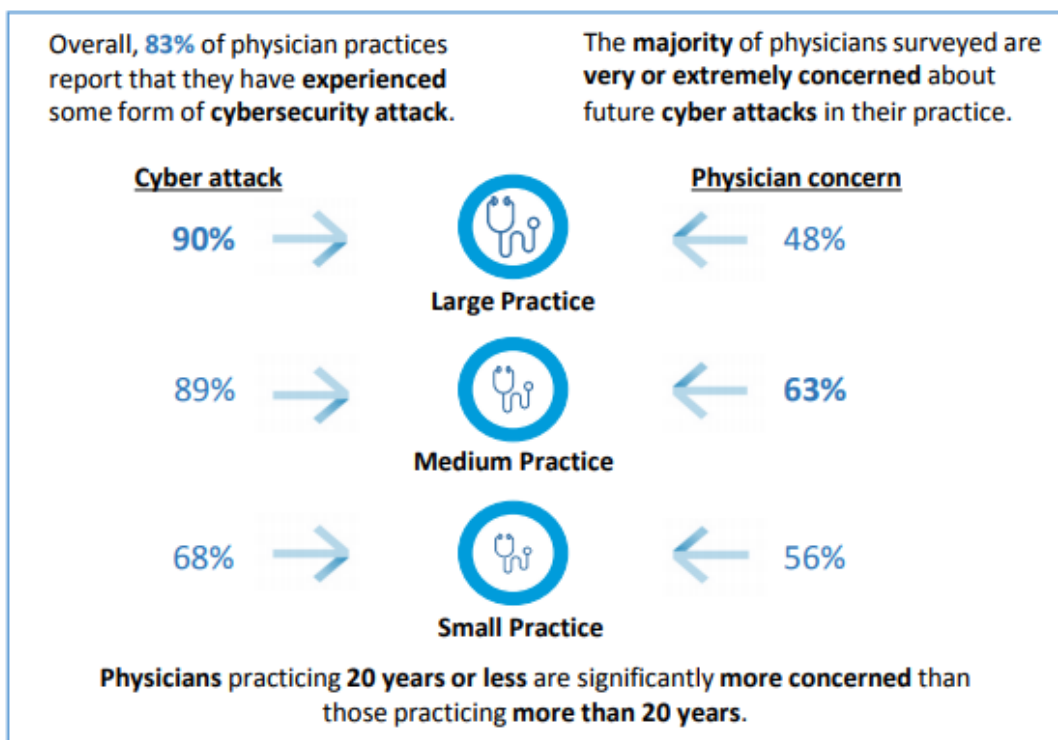
The AMA is deeply concerned that our nation's health care providers have been insufficiently prepared to help meet the cybersecurity challenges of an increasingly digital health care system. We firmly believe that this is a national priority and that physicians and other health care providers need tools 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.**

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 are interested in receiving tools and resources; 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.¹ The top three cybersecurity concerns that physicians identified were interruption to electronic health records (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.”² 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.

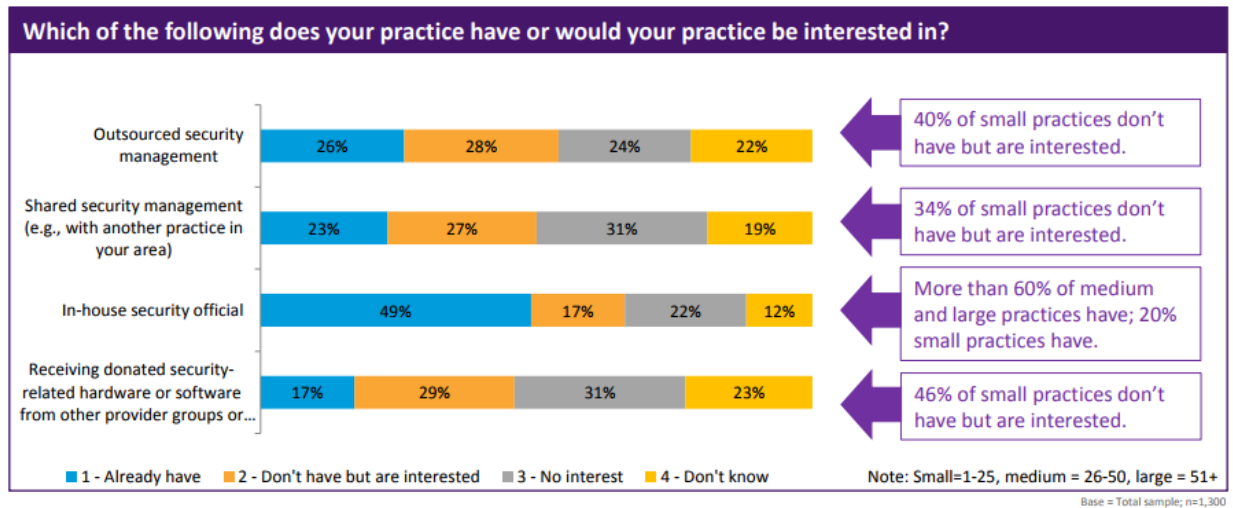


These attacks can jeopardize patient safety and interrupt physician practice operations. Most physician practices experience up to four hours of downtime as a result of cyber attack, but some take almost a full day to resume operations.

¹ AMA, *Medical Cybersecurity: A Patient Safety Issue*, (Dec. 2017), available at <https://www.ama-assn.org/about/medical-cybersecurity-patient-safety-issue>.

² 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>.

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. 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 alternative payment models 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. Moreover, 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.

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 Self-Referral Law, and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners.³

Definitions: In defining cybersecurity, OIG should look to other government agencies. For example, the National Institute of Standards and Technology (NIST) defines cybersecurity to include 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.”⁴

Scope: The AMA believes that non-monetary remuneration should be covered to include items and services in the form of hardware, software, or cybersecurity or training services. This includes upgrades of equipment and software to enhance functionality; license, right to use, and intellectual property; and security education and support (including on-demand help desk and maintenance services). 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. 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.

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

³ 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>.

⁴ NIST, *Glossary of Terms from the Computer Security Resource Center*, available at <https://csrc.nist.gov/Glossary/?term=3817#AlphaIndexDiv> (definition of “cybersecurity”).

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.

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.

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 in order 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.

In order to guard against overutilization, increased federal program costs, corruption of medical decision making, and unfair competition, OIG should consider the following protections:

- Not making the receipt of cybersecurity tools or services a condition of doing business with a donor;

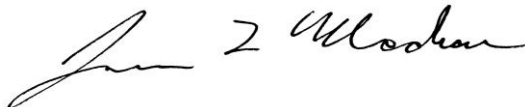
- Not restricting the use of cybersecurity tools or services for any patient regardless of payor;
- Creating a written agreement that is signed by the parties that identifies with specificity about the tools or services provided or shared; and
- Assurance that eligibility to receive donated cybersecurity 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.

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

Conclusion

We appreciate the opportunity to provide our recommendations on new safe harbors. The AMA is committed to engaging with OIG and other stakeholders going forward to identify and inform focused and efficient program integrity measures. We offer our assistance as OIG considers the impact of the fraud and abuse laws on physician participation in innovative payment and delivery models and cybersecurity. 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