AMA
AMERICAN MEDICAL ASSOCIATION

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

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

May 24, 2018

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
United States House of Representatives
2322A Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden and Ranking Member Pallone:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to provide comments and recommendations to address cybersecurity and the use of legacy technologies in health care. The AMA applauds congressional efforts to address the challenges created by legacy technologies in the health care sector.

The AMA is deeply concerned that our nation's health care providers and patients have been insufficiently prepared to meet the cybersecurity challenges of an increasingly digital health care system. Cybersecurity is a national priority and physicians, other health care providers, and patients need tools to secure sensitive patient information in the digital sphere. As clinical adoption of digital medicine tools accelerates with new innovations, and in light of increased public and commercial insurer coverage of digital medicine tools and services, there is increased urgency to advance policies that remedy vulnerabilities in cybersecurity.

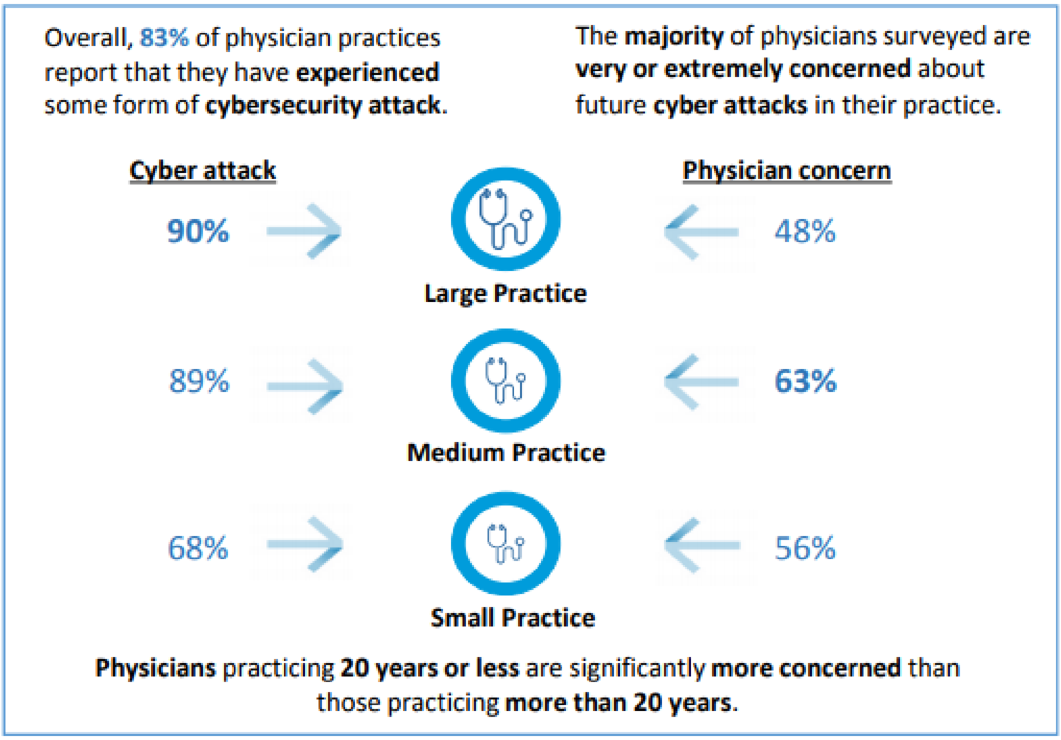
Congress and the Administration should address the challenges of legacy technologies because: (1) cybersecurity is a patient safety issue; (2) cyber attacks are inevitable; (3) physicians are interested in receiving tools and resources to assist them in their cybersecurity efforts; and (4) the health 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 first of its kind 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

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

safety issue. Thus, in making the cost-benefit analysis in identifying, managing, and fixing the vulnerabilities of legacy technology, the first consideration must be the potential harm to patients and interruption of their care.

Cyber attacks are inevitable and physicians are concerned about future attacks. 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. Unfortunately, legacy technology only adds to the overall cyber vulnerabilities of a medical practice.

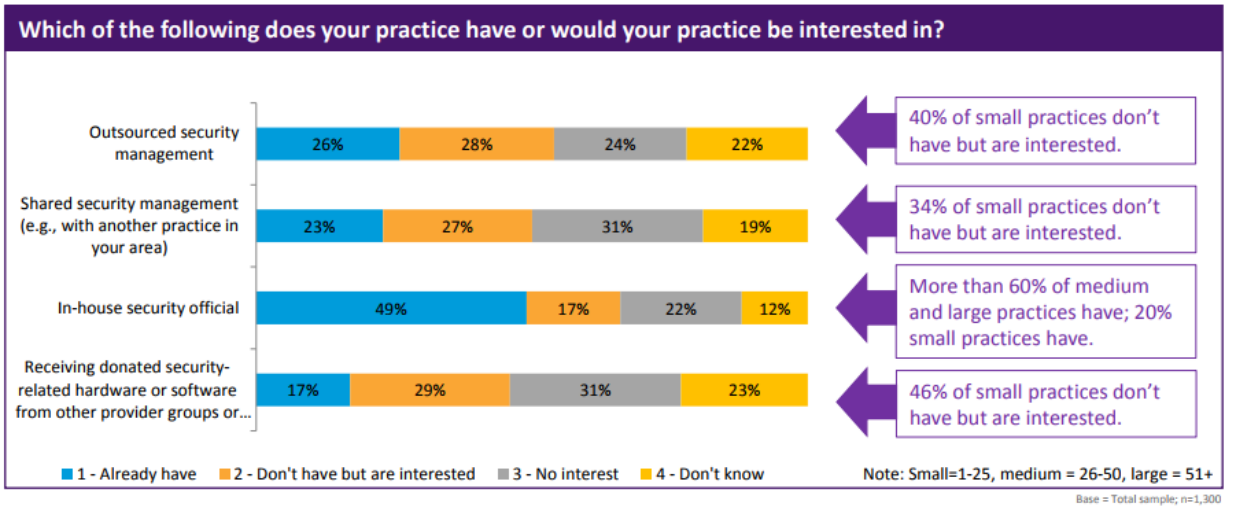


Overall, 83% of physician practices report that they have **experienced** some form of **cybersecurity attack**.

The **majority** of physicians surveyed are **very or extremely concerned** about future **cyber attacks** in their practice.

Physicians practicing **20 years or less** are significantly **more concerned** than those practicing **more than 20 years**.

Physician practices spend a substantial amount on cybersecurity. For example, as noted in the AMA's cybersecurity study's 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. Specifically, physicians are interested in receiving tools and resources to increase their cyber hygiene, and the AMA is advocating for ways to help make these tools and resources available to physicians without violating the Stark Law or Anti-Kickback Statute.



40% of small practices don't have but are interested.

34% of small practices don't have but are interested.

More than 60% of medium and large practices have; 20% small practices have.

46% of small practices don't have but are interested.

Note: Small=1-25, medium = 26-50, large = 51+

Base = Total sample; n=1,300

Finally, cybersecurity and legacy technology impact 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.

Recommendations

The AMA strongly urges adoption of public policy that emphasizes greater transparency, physician educational resources, more equal distribution of risk of liability and government enforcement between physicians and technology vendors and manufacturers, and positive incentives to encourage cybersecurity best practice adoption.

Focus on Patient Care

Physicians and the patient's health care team should be focused on providing patient care. Yet, increasing administrative responsibilities—due to regulatory pressures and liability concerns—reduce the amount of time physicians and the health care team can spend delivering direct patient care. Physicians understand how to use these technologies in order to make more accurate diagnoses and provide better treatments to patients. However, with legacy technologies, physicians generally do not know and may have no way of knowing what software or hardware exists within the medical technologies on which they rely to provide vital medical care.

Physicians are not cybersecurity experts and typically do not have the training or subject matter expertise to understand the technological nuances surrounding cybersecurity. Instead, physicians, the extended health care team, and patients are still learning and gradually adopting basic cybersecurity measures and practices. For example, when providing education and outreach to physicians, AMA focuses on **basic security** tools about protecting mobile devices, keeping software up to date, installing anti-virus software, securing Wi-Fi networks, and setting secure passwords.

Transparency

Physicians are confronted with unanticipated charges by technology manufacturers and EHR vendors for cybersecurity software updates and patches. These technology vendors need to be more transparent with and proactive about disclosing costs to physicians upfront, ability to update and patch, the expected timeframe of manufacturer support of the technology, and where in the product development lifecycle a specific product sits. Furthermore, since most physicians are not technology experts, product information should include not only technical documentation, but also layman's language clearly outlining potential risks and/or benefits of the technology to patient health and safety. This is the minimum amount of information physicians need to optimize cybersecurity and make informed choices. Specifically, the information will position physicians to select EHR vendors and manufacturers that will support the practice's cybersecurity needs.

Software Bill of Materials

The AMA strongly supports a software bill of materials (SBOM) for all technologies currently in use. A SBOM include components (e.g., equipment, software, open source, materials) and any known risks associated with those components to enable health care providers to more quickly determine if they are impacted by a cybersecurity threat.

As the U.S. Department of Health & Human Services Cybersecurity Task Force Report (Report) states, a SBOM is "key for organizations to manage their assets because they must first understand what they have on their systems before determining whether these technologies are impacted by a given threat or vulnerability."[2] In the event that a threat or vulnerability is exploited, a SBOM may help a physician prioritize what vulnerability is the biggest threat to patient care. Understanding the supply chain of software, obtaining a SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.

Furthermore, when a security breach occurs, a SBOM is critical in identifying and describing open source and third-party software components to allow for a quick response. A SBOM may also contribute to a physician's ability to better conduct a thorough security risk analysis—a requirement of both the Health Information Portability and Accountability Act (HIPAA) and the EHR Incentive Programs—because physicians will be able to "assess the risk of medical devices

[2] 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.

on their networks, confirm components are assessed against the same cybersecurity baseline requirements as the medical device, and implement mitigation strategies when patches are not available." The Report further notes that, "[t]o date, this practice has not been widely adopted."

Physician Education

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

In providing education on cybersecurity and the risks associated with using legacy technologies, vendors and manufacturers should explain why technologies need to be updated in plain English, using standardized formats and a consistent articulation of level of risk. When a vulnerability or threat is detected, such information should be communicated not in a highly technical manner, but rather should be automated to greatest extent practicable, identify the level of risk, be articulated through the concept of patient safety where possible, and include specific steps to address vulnerabilities. As described above, physicians also need to understand what software and hardware exist within their medical technologies.

Copyright Issues

Most medical technologies come with some form of software from the manufacturer or vendor. This implicates copyright law, which places importance on the contractual terms relating to a copyright owner's protected rights in that software. The use of this software can be subject to license agreements between the vendor and consumer—in this case, a provider purchasing technology. License agreements generally include disclaimers of warranties and any defects and limit the remedies available to consumers. This can enable vendors to shift liability for a software defect onto clinicians and subject patients to higher levels of risk.

Equitable Distribution of Risk

Relative to vendors and manufacturers, physicians are not the most knowledgeable of potential cybersecurity risks, are not the best situated to mitigate risks, and are not necessarily experts in understanding the underlying technological specifications. Nonetheless, it is physicians who are at risk of liability and potential government enforcement actions.

When considering implementing policy changes to improve cybersecurity surrounding legacy technologies, the Committee should consider properly allocating the risk across all involved parties. It should align incentives so those best positioned to have knowledge of risks and best positioned to minimize harm through design, development, validation, or implementation are incentivized to do so. Manufacturers and EHR vendors should proactively minimize risk to patients and continue updating and patching technologies as new vulnerabilities emerge. As with providers, manufacturers and EHR vendors should share accountability for protecting patient data and maintaining data integrity. Greater transparency and proactive measures should reduce potential liability. Potential solutions could include creating affirmative defenses that reward transparency, compulsory insurance with a compensation fund, or a more holistic approach to enterprise liability that includes manufacturers and vendors. Furthermore, regardless of risk allocation, gag clauses to prevent public reporting of adverse events are contrary to public policy and must be deemed illegal.

Small Practice Considerations

Small physician offices that do not have stand-alone information technology (IT) departments need extra help in navigating cybersecurity challenges and dealing with legacy technologies. Small practices may also be priced out of participation in alternative payment models if they cannot afford to access cybersecurity tools and expertise or update/replace legacy technologies. Unfortunately, cyber hackers now have more potential entry points to exploit vulnerabilities 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 or legacy technologies. Even if a physician's office houses relatively few health care records, it may be connected to other health systems with significantly more data. Importantly, 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.

Positive Incentives

The AMA encourages Congress and the Administration to help reframe the conversation from punitive requirements to an opportunity for positive incentives to encourage cybersecurity activities that will protect practice continuity and patient information. Two main incentives are creating a cybersecurity anti-kickback safe harbor/Stark exception and improvement activities (IAs) for the Medicare Quality Payment Program (QPP) that promote good cyber hygiene.

The AMA recently requested that the Office of Inspector General (OIG) create a safe harbor that allows for the sharing of cybersecurity items and services with detailed suggestions into the structure of a potential safe harbor including definitions, scope, donors, recipients, value of technology, and appropriate safeguards.[3] Overall, the AMA stresses that any cybersecurity anti-

[3] AMA, *Letter to OIG in Response to Solicitation of Safe Harbors*, (Feb. 2018), *available at* https://searchlf.ama-assn.org/undefined/documentDownload?uri=%2Funstructured%2Fbinary%2Fletter%2FLETTERS%2F2018-2-26-Letter-to-Levinson-re-Draft-OIG-Annual-Solicitation.pdf.

kickback safe harbor or Stark exception 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. This concept is reflected in the Report's Recommendation 1.5, which "strongly encourage[s] Congress to evaluate an amendment to [the Stark Law and Anti-Kickback Statute] specifically for cybersecurity software that would allow health care organizations the ability to assist physicians in the acquisition of this technology, through either donation or subsidy." Although OIG has the regulatory authority to create an anti-kickback safe harbor, the Centers for Medicare & Medicaid Services (CMS) must show no program or patient abuse in creating Stark exceptions. This Stark standard is difficult for CMS to meet and has caused other proposed regulatory Stark exceptions to fail. Thus, Congress may need to provide this positive incentive to promote cybersecurity throughout the health care system.

The AMA supports efforts to promote health IT throughout the Merit-based Incentive Payment System (MIPS) track of the QPP. The AMA has urged CMS to expand this recognition beyond the bonus points that a clinician can receive in the Advancing Care Information category (recently renamed the Promoting Interoperability category) within MIPS for using certified EHR technology to accomplish IAs. Namely, CMS should add IAs that give credit to physicians who use health IT—both certified and non-certified—to enhance patient safety, beneficiary engagement, and security of health information. For example, given increases in cyber threats, CMS should reward clinicians who are proactive in ensuring the safety of their electronic patient information, including recognizing actions that HIPAA may not address, by implementing cybersecurity risk management practices, adopting voluntary cybersecurity best practices, and improving patient safety through cybersecurity hygiene education.

Thank you for the opportunity to provide comments and recommendations on cybersecurity and the use of legacy technologies in health care. We look forward to working with the Committee in addressing these challenges and potential solutions to promote patient safety, to protect practice continuity, and to appropriately manage risk.

Sincerely,

James L. Madara, MD