

March 20, 2019

The Honorable Mark Warner
United States Senate
703 Hart Senate Office Building
Washington, DC 20510

Dear Senator Warner:

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 vulnerabilities in the health care system. The AMA applauds congressional efforts to address this challenge and to develop a national strategy that improves the safety, resilience, and security of the health care industry.

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.

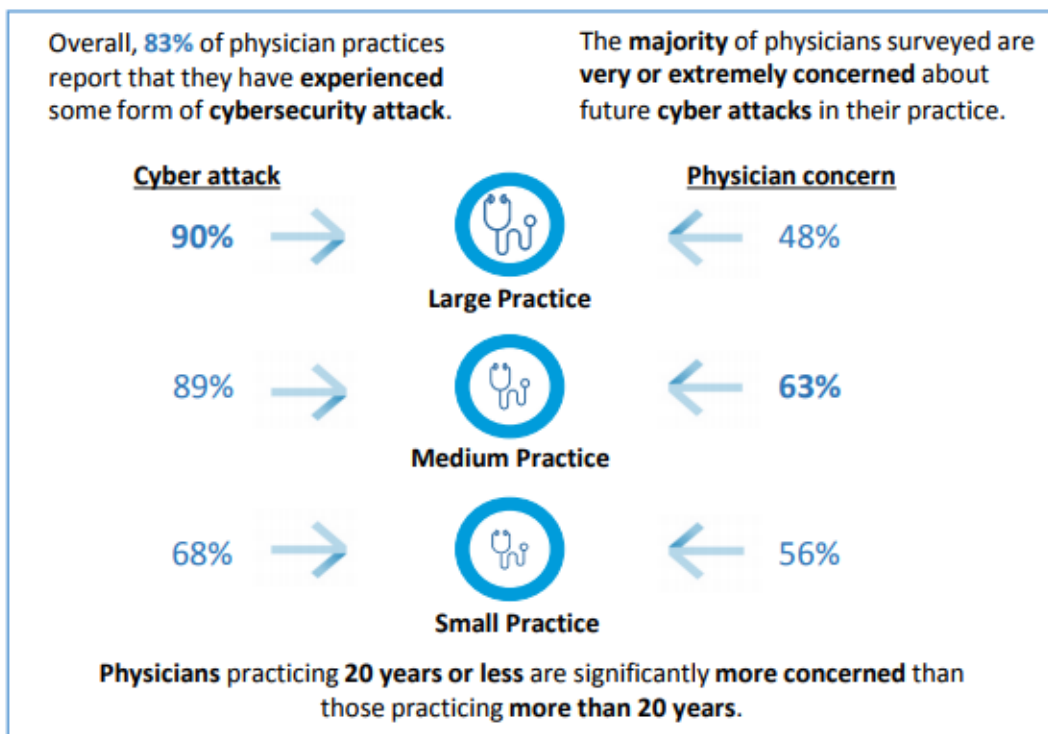
Congress and the Administration should address cybersecurity vulnerabilities because: (1) cybersecurity is a patient safety issue; (2) cyber attacks are inevitable and increasing; (3) physicians are interested in receiving tools and resources to assist them in their cybersecurity efforts; and (4) the 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 safety issue. Others in the industry have recognized the threat to patient safety that can result from weak cybersecurity controls: the 2017 U.S. Department of Health and Human Services' (HHS') Health Care Industry Cybersecurity Task Force Report (Task Force Report) notes that for the health care industry, "cybersecurity issues are, at their heart, patient safety issues."² Thus, in developing a national cybersecurity strategy for the health care industry, the first consideration must be the potential harm to patients and interruption of their care.

¹ AMA, [Medical Cybersecurity: A Patient Safety Issue](#), (2017).

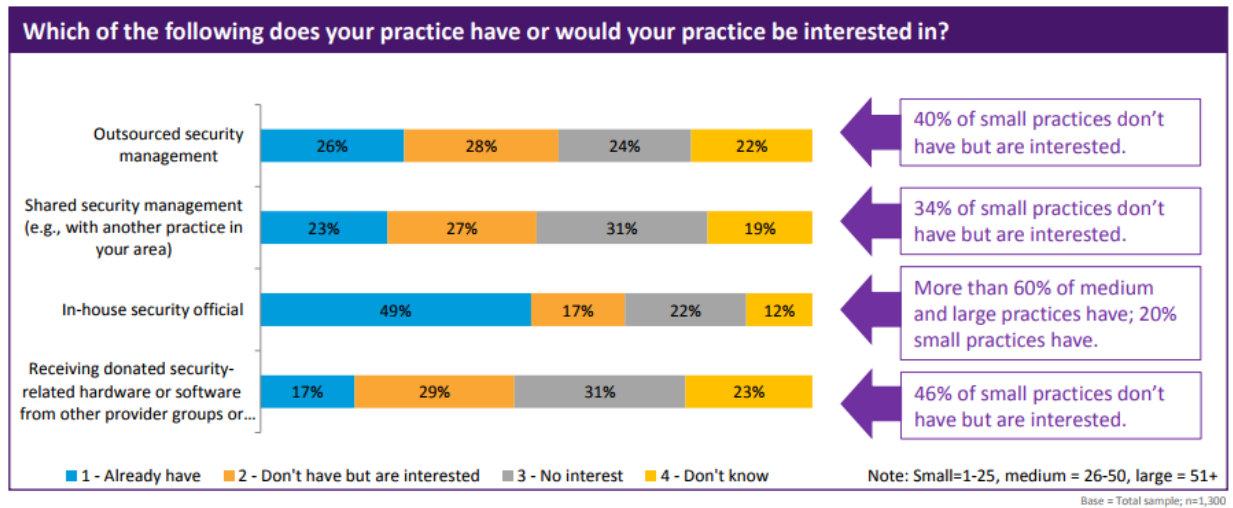
² [HHS Cybersecurity Task Force Report](#).

Cyber attacks are inevitable and physicians are concerned about future attacks. Last year was a record-breaking year for health care data breaches and cyber attacks will continue to increase as health systems and other covered entities continue to amass enormous quantities of valuable health data using new health information technology (IT).³ 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.



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.

³ HIPAA Journal, [Analysis of 2018 Healthcare Data Breaches](#), (Jan. 2019).



Finally, cybersecurity impacts 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.

Proactive Steps

Physicians and the patient's health care team should be focused on providing patient care. Physicians need to understand how to use certain technologies to make more accurate diagnoses and provide better treatments to patients. However, 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, the 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.⁴ Thus, instead of focusing on real-time information on the patch status of all connected systems, the AMA's educational efforts are directed at identifying what patches mean and ensuring that operating system and web browser updates automatically download.

Moreover, the AMA recently released a Digital Health Implementation Playbook that lays out a path to implement new digital health solutions including key steps, best practices, and resources to accelerate and

⁴ AMA resources include [How to Improve Your Cybersecurity Practices](#); [Checklist for Office Computers](#); and [Protect Your Practice and Patients from Cybersecurity Threats](#). These resources are also attachments to this letter.

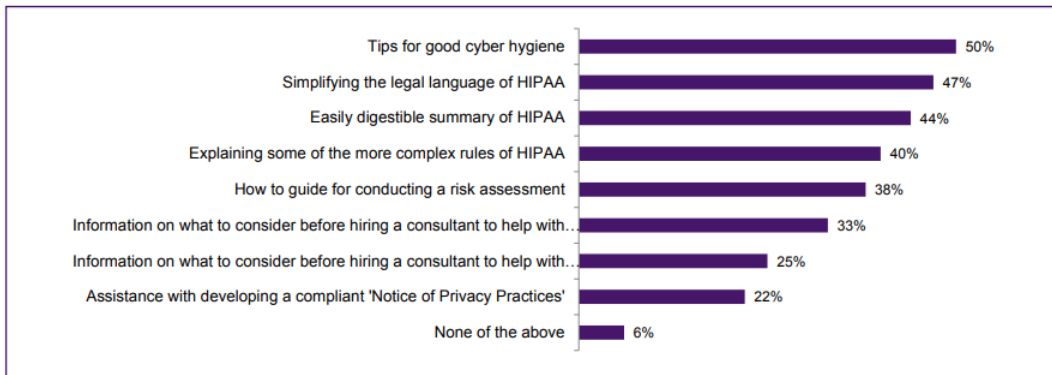
achieve digital health adoption.⁵ The Playbook includes overview information on how to collect patient health information using devices, trackers, and sensors to improve the management of chronic disease. It also includes a Cybersecurity 101 Section discussing cybersecurity concerns when implementing digital health into a practice and provides a sample vendor-information request form including a section on data security privacy that asks about mitigating cyber threats.

Furthermore, the AMA pioneered Xcertia, a joint mHealth app collaborative, with DHX Group, American Heart Association, and Healthcare Information and Management Systems Society (HIMSS). Xcertia is focused on developing and disseminating mHealth app guidelines that can drive the value that mHealth apps bring to the market and the confidence that physicians and consumers can have in these apps and their ability to help people achieve their health and wellness goals. These guidelines—which are currently out for public comment—include app security guidelines that assess whether an application is protected from external threats and maintain the integrity, availability, confidentiality, and resilience of the data.⁶ The guidelines aim to identify and reduce cybersecurity vulnerabilities for mHealth app developers.

Security Awareness and Technical Capacity

The main tool physician offices use to develop security awareness is through privacy and security education and training. This content can be generated by a variety of parties, though the AMA survey identified that physicians turn to their health IT vendor the most (37 percent). The 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.”⁷ 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, as seen in the graph below.

Security training for physicians



⁵ AMA, [Digital Health Implementation Playbook](#), (2018).

⁶ Xcertia, [App Security Guidelines & Survey](#), (2019).

⁷ 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>.

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 with a consistent articulation of level of risk. Physicians should also be provided information on how to identify the altered performance of devices. Cyberattacks may change the normal function of a device, and without knowing what to look out for, physicians may not know when a product is malfunctioning. This is particularly important when physicians rely on data from medical devices to monitor or treat patients. When a vulnerability or threat is detected, such information should be communicated not in a highly technical manner, but rather should be automated to the greatest extent practicable, identify the level of risk, be articulated through the concept of patient safety where possible (physicians respond strongly when cybersecurity is viewed through this lens), and include specific steps to address vulnerabilities. As described above, physicians also need to understand what software and hardware exist within their medical technologies, using a software bill of materials (SBOM, discussed further below).

With technical capacity, the AMA is concerned that small practices will be left out of the discussion. Small physician offices that do not have stand-alone IT departments need extra help in navigating cybersecurity challenges and dealing with legacy technologies. Only 20 percent of small practices have internal security officers, so they typically rely on health IT vendors for security support.⁸ 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.

Federal Efforts and Recommendations

The AMA believes that the federal government is working to establish an effective national strategy to reduce cybersecurity vulnerabilities in the health care sector. However, more can be done through greater transparency including an SBOM, equitable distributing risk among the health care industry, and reframing the conversation to focus on positive incentives.

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, their 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 layperson'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

⁸ See AMA Survey.

information will position physicians to select EHR vendors and manufacturers that will support the practice's cybersecurity needs.

The AMA strongly supports the creation of SBOMs for all technologies currently in use. An SBOM includes a list of components (e.g., equipment, software, open source, materials) in a given technology 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 Task Force Report states, an 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.”⁹ If a threat or vulnerability is exploited, an SBOM may help a physician prioritize what vulnerability is the biggest threat to patient care. Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.

Furthermore, when a security breach occurs, an SBOM is critical in identifying and describing open source and third-party software components to allow for a quick response. An 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 Promoting Interoperability Programs—because physicians will be able to “assess the risk of medical devices 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.”¹⁰ The Task Force Report further notes that, “[t]o date, this practice has not been widely adopted.”¹¹

Equitable Distribution of Risk

Relative to vendors and manufacturers, physicians generally lack knowledge 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, and 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.

⁹ Task Force Report, p. 29.

¹⁰ Id.

¹¹ Id.

Positive Incentives

The AMA also 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. Three main incentives are creating a cybersecurity anti-kickback safe harbor and Stark (physician self-referral) exception, developing improvement activities (IAs) for the Medicare Quality Payment Program (QPP) that promote good cyber hygiene, and permitting multiple paths to the HIPAA Security Rule.

The AMA 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.¹² Overall, the AMA stresses that any cybersecurity anti-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 Task Force 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 submitted several IA proposals intended to increase patient safety, enhance privacy and security of patient records, and provide education to patients around the use of health IT during CMS' call for measures in both 2017 and 2018, yet CMS has not accepted any of the AMA's IA proposals for inclusion in its IA Inventory. The AMA believes that these IAs are crucially important especially as health information becomes increasingly valuable on the black market.¹³ CMS requires physicians to use health IT to fully participate in the QPP, yet provides insufficient incentives to do so in a secure manner despite such efforts being costly, time-consuming, and incredibly important to patient safety. Thus, 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 adopting the following IAs:

- Adopt voluntary cybersecurity practices identified by the security industry and federal government;
- Adopt a cybersecurity framework (e.g., the National Institute of Standards and Technology [NIST]) and identify an implementation process; and

¹² AMA, [Letter to OIG in Response to Request for Information on Valued-Based Care](#), (Oct. 2018); AMA, [Letter to OIG in Response to Solicitation of Safe Harbors](#), (Feb. 2018).

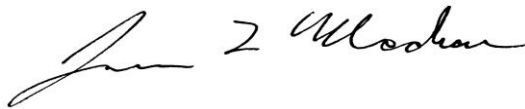
¹³ See Mariya Yao, Forbes, [Your Electronic Medical Records Could Be Worth \\$1000 To Hackers](#) (Apr. 2017).

- Provide written and/or face-to-face education to consumers about privacy and security considerations when electronically accessing health data. This activity will be even more critical considering the patient access rules recently proposed by CMS and the Office of the National Coordinator for Health Information Technology (ONC), which will result in more exchange of health information than ever before.

The AMA appreciates the flexibility of the HIPAA Security Rule's requirements because physician practices are varied and have different security needs, resources, and skill levels. Many practices understand that they need robust plans to ensure their systems and patients are protected, yet struggle with conducting security risk analyses as outlined by HIPAA. Thus, Congress or the Administration should permit "multiple paths to compliance" with HIPAA's Security Rule. Statute or regulations could be revised to state that covered entities that adopt and implement a security framework (such as the NIST Cybersecurity Framework) or take steps toward applying the Health Industry Cybersecurity Practices¹⁴ (the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group) are in compliance with the Security Rule. This modification would help make cybersecurity more understandable and attainable to physicians, particularly those that are most vulnerable due to lack of resources and expertise. The whole health care system—including patients—benefits when protected health information is kept private and secure. The NIST Cybersecurity Framework and the Health Industry Cybersecurity Practices best practices utilize industry experts to identify the most pressing risks and develop safeguards to help to address these risks. HHS Office of Civil Rights' adoption of this change would empower physicians who think cybersecurity is an insurmountable task and may not even recognize that good cyber hygiene is within their reach.

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

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

¹⁴ HHS Office of the Assistant Secretary for Preparedness and Response, [Health Industry Cybersecurity Practices](#), (2018). By way of background, in 2015, Congress passed the Cybersecurity Act of 2015 (CSA), which includes Section 405(d), Aligning Health Care Industry Security Approaches. In 2017, HHS convened the CSA 405(d) Task Group, leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. The Task Group is comprised of a diverse set of over 100 members representing many areas and roles, including cybersecurity, privacy, healthcare practitioners, Health IT organizations, and other subject matter experts. The Health Industry Cybersecurity Practices they developed aim to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. The publication seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes.