



JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

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

December 1, 2022

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 in response to the November 2022 white paper entitled “Cybersecurity is Patient Safety: Policy Options in the Health Care Sector.” The AMA applauds Congress’ ongoing leadership pertaining to the issue of cybersecurity and for soliciting responses from key stakeholders related to unique policy approaches. The AMA welcomes Congressional efforts to address cybersecurity and develop a national strategy that improves the safety, resilience, and security of the health care industry.

Our organization 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. This is at a time when several federal policies require the sharing of highly sensitive medical information without first establishing a solid foundation of data security and privacy to protect patients. 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 remains a sense of urgency to advance policies that remedy vulnerabilities in cybersecurity.

There are a multitude of reasons for Congress, as well as the Biden Administration, to address cybersecurity including: 1) cybersecurity is a patient safety issue; 2) cyberattacks are inevitable and increasing; 3) physicians are interested in receiving tools and resources to assist them in cybersecurity efforts; and 4) the health care sector exchanges health information electronically more than ever before, putting the entire health care ecosystem at risk. Despite the demand for legislative action, as you begin the larger process of formulating a bill, we encourage any policy changes be developed with the recognition that physicians, especially small and rural practices, possess limited resources to implement these important cybersecurity policies.

Our more in-depth responses to the various sections of the white paper are found in the attached chart. The detailed comments address the vast majority of the components of the three major chapters, specifically “Improving Federal Leadership and Our National Risk Posture,” “Improving Health Care Providers’ Cybersecurity Capabilities through Incentives and Requirements,” and “Recovery from Cyberattacks.”

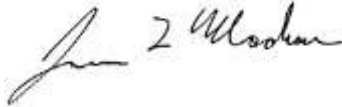
The Honorable Mark Warner

December 1, 2022

Page 2

The AMA appreciates the opportunity to provide comments and recommendations in response to “Cybersecurity is Patient Safety: Policy Options in the Health Care Sector.” We look forward to working with you in addressing these challenges and potential solutions to promote patient safety, protect practice continuity, and appropriately manage risk. Should you have additional questions, please do not hesitate to contact Chris Sherin, Assistant Director, Division of Congressional Affairs, via email at Christopher.Sherin@ama-assn.org.

Sincerely,

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

James L. Madara, MD

Enclosure

AMA Detailed Comments on “Cybersecurity is Patient Safety: Policy Options in the Health Care Sector”

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
<p>1.1 HEALTH CARE CYBERSECURITY LEADERSHIP WITHIN THE FEDERAL GOVERNMENT</p>	<p>3. Should the 405(d) Program continue to be the “hub” of HHS and federal government partnership with industry?</p> <p>3a. What other agencies should be part of such an effort, and how should they coordinate?</p> <p>3b. Does the 405(d) Program need additional resources to ensure it can continue to develop and disseminate its work? How do we effectively measure the efficacy of 405(d) in order to evaluate what is the appropriate level of additional resources?</p>	<p>The AMA remains highly supportive of section 405(d) of the Cybersecurity Act of 2015 and the associated resources promulgated under this law. The AMA has publicized these resources on its own cybersecurity page and is particularly grateful for its attention to providing resources for small physician practices. AMA members and the House of Medicine have expressed increased concerns over cybersecurity in recent years, and the 405(d) resources have been timely, informative, and user-friendly. Additionally, the U.S. Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) recently launched a new website to help physicians and their medical practices be better informed about potential cyber threats. This new site lists several resources, including threat briefs with best practices and information on COVID-19 related cyber threats and sector alerts with high-level information to assist non-technical audiences. We also often refer physicians to the website of the Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group, which is comprised of experts across the health care sector, many of whom are actively monitoring health care threats and trends particularly relevant to the field.</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
<p>1.3 HEALTH CARE SPECIFIC GUIDANCE FROM NIST</p>	<p>1. What should be included in a health care cybersecurity framework? Is sector-specific guidance from NIST for the health care sector necessary?</p> <p>2. Is the current guidance from NIST sufficient? Has your organization or members of your organization implemented the recommendations in the Cybersecurity Framework? If not, why?</p>	<p>Physician practices spend a substantial number of monetary resources on cybersecurity infrastructure and solutions. 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. The AMA further notes that, per the AMA-Accenture 2017 survey of 1,300 physicians, only one in five small physician practices have an in-house security official. This is one strong indication that small practices are likely in need of extra help navigating basic cybersecurity challenges that may exist by virtue of budgetary constraints, knowledge-based limitations, and limited staff resources. The federal government needs to empower physicians to actively manage their security posture without straining their limited information technology (IT) budgets.</p> <p>Therefore, with respect to specific guidance from the National Institute of Standards and Technology (NIST) cybersecurity framework, it is critical that maintenance of flexibility be at the forefront of these recommendations. It is vitally important to remember that a solo practitioner has very different resources than a large health system. The AMA strives to help physicians navigate a complex future where non-traditional players, such as cyberhackers, expose their practices and their patients to risk. Yet, while discussions of cybersecurity typically include perspectives of government, health</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>IT vendors, and large health and hospital systems, the physician voice is relatively unheard. The AMA recommends that NIST and others in the cybersecurity space contemplate ways to make cybersecurity best practices affordable, attainable, and approachable for physicians without extensive health IT knowledge or experience. This is particularly critical for physicians as they have primary responsibility over the health care cybersecurity role at their respective organization. Finally, AMA supports health care specific cybersecurity guidance or playbooks remain voluntary as to not put undue regulatory or financial burdens on physician practices.</p>
<p>1.4 MODERNIZING HIPAA TO ADDRESS CYBER THREATS</p>	<p>1. Is it appropriate to address both privacy and security within a single enforcement regime or are the risks, solutions, and institutional competencies sufficiently distinct to warrant separate regulatory regimes?</p>	<p>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’ data are protected yet struggle with conducting security risk analyses as outlined by HIPAA. Privacy and security are inextricably linked and the concerns that are prevalent in the cybersecurity realm are even more manifest with respect to privacy, HIPAA, and the interoperability regulations. Thus, Congress or the Administration should permit “multiple paths to compliance” with HIPAA’s Security Rule. The AMA strongly supported the passage of Public Law (PL) 116-321 (HR 7898 HIPAA Safe Harbor Law), which addressed health information technology provisions related to cybersecurity and information blocking. Congress</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>should consider additional opportunities to extend the flexibility found in PL 116-321. For instance, while the law offers protection to physicians under certain circumstances, it does not provide a true safe harbor. A typical safe harbor shields an entity from liability when certain conditions are met. PL 116-321, however, only allows Office for Civil Rights (OCR) leniency in assessing the breach. The AMA recommends Congress strengthen the law and create a true Safe Harbor for physicians’ medical practices when certain conditions are met.</p> <p>AMA does not support the expansion of HIPAA to cover app developers. Instead, the Office of the National Coordinator for Health Information Technology (ONC) should create commonsense policies that give patients information about what apps do with the health data they receive. To help provide a minimal amount of transparency to patients about how a health app will use their health information, ONC should implement a basic privacy framework requiring certified EHR vendor APIs to check an app’s “yes/no” attestations to:</p> <ol style="list-style-type: none"> 1. <i>Industry-recognized development guidance</i> (e.g., Xcertia’s Privacy Guidelines); 2. <i>transparency statements and best practices</i> (e.g., Mobile Health App Developers: FTC Best Practices/AMA Privacy by Design); and 3. <i>a model notice to patients</i> (e.g., ONC’s Model Privacy Notice).

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>Requiring an API check for an app developer attestation would not be a significant burden on EHR vendors (which develop APIs) and apps would not be prevented from connecting to an EHR even if they attest “no” to the three checks. Accordingly, this framework is low-touch for EHR and app developers and does not require special effort by patients, yet it would provide some level of transparency to patients and physicians. Furthermore, the framework would serve to assist the FTC in the event of an investigation or enforcement action of deceptive or unfair trade practices if the app strays from what it tells consumers. In addition, we strongly urge OCR to coordinate with the ONC, given the privacy overlay with the information blocking rule, as well as with the NIST. NIST has developed valuable resources that provide guidance on cybersecurity trends and recommend best practices to individuals and organizations across the country, including many physician practices. NIST recognizes that cybersecurity practices will vary across organizations, depending on levels of technical understanding, financial and human resources, and risk tolerance. This flexibility allows entities to customize how they adopt and implement a cybersecurity framework and is critical in the health care space where a solo practitioner has very different resources than a large health system.</p>
<p>1.5 STARK LAW AND ANTI-KICKBACK STATUTE</p>	<p>2. Are there providers for whom even the safe harbor/exception introduces too much legal risk for the provider, leading to not taking advantage of cooperation that other providers with a higher risk tolerance are comfortable with? Or are the regulations clear enough even for the most risk</p>	<p>The AMA agrees that the Stark law and Anti-kickback statutes are important laws that work to prevent waste, fraud, and abuse in the Medicare program. With respect to carving out exceptions to these laws and not preventing stakeholders in legitimate partnerships from accepting cybersecurity donations</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
	<p>averse providers? Can Congress amend the statute to make it clearer and more effective regarding cybersecurity partnerships?</p> <p>3. Are there downsides to allowing health care providers to accept donations of cybersecurity and IT products, such as encouraging health care organizations to externalize responsibility and cost for IT security?</p>	<p>that would protect the health care system collectively and not introduce financial risk in the Medicare program, the AMA offers the following comments in select issue areas:</p> <p>Value Based Care</p> <p>The AMA supports modified definitions of value-based purpose and the inclusion of infrastructure investment and operations necessary to redesign care delivery. Yet, we are opposed to precluding some or all protection under safe harbors for arrangements between entities that have common ownership. This type of restriction precludes protection for care coordination arrangements within a group practice or among entities in integrated health care systems that could otherwise qualify for proposed safe harbor protections.</p> <p>The AMA also believes that remuneration in the form of cybersecurity items or services could meet the definition of the “coordination and management of care for a target patient population.” For example, cybersecurity items or services may be needed to help share information between two or more value-based enterprise (VBE) participants. Value-based arrangements 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 (APMs) if they cannot access affordable cybersecurity tools.</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>Moreover, cybersecurity items or services could also improve the quality of care for a target patient population by ensuring that information is shared securely and without alterations. While we believe that a majority of cybersecurity items or services would receive protection under a cybersecurity safe harbor at 1001.952(jj), hardware and other infrastructure investments for cybersecurity services are not always covered under the cybersecurity safe harbor. Therefore, the AMA supports Congress passing legislation clarifying this particular safe harbor that covers all types of cybersecurity hardware and other infrastructure investments.</p> <p>While it is important to note that CMS does not define “coordinating and managing care,” we do have concerns as to how the HHS Office of the Inspector General (OIG) has defined the term. We disagree with the current definition of “coordinating and managing care” that requires patient care activities and sharing information to achieve safe and more effective care for the target patient population. While the goal of coordinating care should be to achieve more effective care, requiring constant achievement is not practical in the practice of medicine. The nature of medical practice is constantly evolving and responding to emergent infectious diseases and natural disasters that may negatively impact outcomes or necessarily increase costs. In these instances, physicians may not be able to achieve more effective care through no fault of their own. The AMA has urged OIG to recognize this reality and define “coordination and management of care” to</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>mean “the deliberate organization of patient care activities and sharing of information between two or more VBE participants or VBE participants and patients, tailored to improving the health outcomes of the target patient population, in an attempt to achieve safer and more effective care for the target patient population.” As a result, this is another area where Congress could explore statutory changes to facilitate greater expansion of cybersecurity within value-based care.</p> <p>Electronic Health Records Items and Services</p> <p>The AMA supports past efforts by CMS to expand the EHR safe harbor exception to expressly include cybersecurity software and services. This expansion makes it clear that an entity donating EHR software and providing training and other related services may also donate related cybersecurity software and services to protect the EHR.</p> <p>Cybersecurity Technology and Related Services</p> <p>The AMA strongly supports the cybersecurity technology and related services exception. 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</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>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. We believe efforts like the cybersecurity technology and related services exception in the amendments to the Stark Rule and Anti-Kickback Statute, help address these challenges and develop a national strategy that improves the safety, resilience, and security of the health care industry.</p> <p>The AMA is generally supportive of the definition of “cybersecurity” within the cybersecurity technology and related services exception. We believe, however, that CMS should also include the process of protecting information by “identifying” and “recovering” from cyber-attacks. This important clarification is an additional area for Congress to consider.</p> <p>By adding “identifying” and “recovering”, the definition of cybersecurity would include the entire lifecycle of a cyber-attack. The addition of “identifying” would include understanding the business context, the resources that support critical functions, and the related cybersecurity risks, enabling an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. The addition of “recovering” would allow for back-up services to be provided which supports reestablishing cybersecurity based-on continuous backups, failover, and reduce the impact of ransomware extortion. The AMA already believes that these concepts are protected under the</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>exception; however, Congress explicitly referencing “identifying” and “recovering” in the definition of cybersecurity will help highlight the importance of these functions.</p> <p>The AMA, however, is opposed to a definition of cybersecurity that is tailored to the health care industry. A broader, industry-agnostic definition is more appropriate because cybersecurity is a fluid, ever-changing concept. Thus, a narrower definition would increase the likelihood of unintentionally limiting donations and of the definition becoming obsolete over time.</p> <p>Accordingly, the AMA recommends that the definition of “cybersecurity” should be the “process of protecting information by <u>identifying</u>, preventing detecting, responding to, and <u>recovering from</u> cyber-attacks.”</p> <p>The AMA appreciates that the intent of the exception is to be agnostic to specific types of non-hardware cybersecurity technologies. We believe that non-monetary remuneration should be covered to include items in the form of software and hardware. The scope of covered items and services would also include all hardware security appliances because many cybersecurity software products require the use of a specific hardware device to operate. Security appliances are purpose-built hardware appliances that are designed to protect computer networks from unwanted traffic and bolster the network’s cybersecurity. For example, an intrusion detection</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>system (IDS) is a device that monitors a network or systems for malicious activity. Some IDS products have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system (IPS). Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPS are necessary additions to the security infrastructure and contribute to a network’s overall cybersecurity. Accordingly, non-monetary remuneration should include items in the form of software and all hardware.</p> <p>The AMA also supports the exception to be limited to donated technology and services that are necessary and used predominantly to implement, maintain, and reestablish effective cybersecurity. Yet, Congress should explore legislative changes to include continuous monitoring and log management software. Additional services include e-mail protection, endpoint protection, access management, data protection and loss prevention, asset management, network management, vulnerability management, incident response, medical device security, and cybersecurity policy development. These types of tools can help identify and detect cyber-attacks.</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>The AMA also supports cybersecurity education services and services associated with performing a cybersecurity risk assessment or analysis as remaining protected under this exception. These services are essential to preventing future cyber-attacks.</p> <p>Finally, the AMA urges Congress to pass legislation that removes the “deeming provision,” which requires donors or recipients to demonstrate that donations are necessary and predominantly used to implement, maintain, or reestablish effective cybersecurity, from the cybersecurity technology and related services exception. This deeming provision adds unnecessary burden, complicates the policy, and does not provide any additional meaningful protection against fraud or illegal remuneration. While the deeming provision does require compliance with a particular framework or set of standards, AMA remains concerned about how a donor and recipient could practically demonstrate “deeming” compliance and the additional burden associated with trying to demonstrate reasonable conformance to a widely recognized cybersecurity framework or set of standards. Physicians continue to struggle with answering questions like what “reasonable conformance” looks like and when a framework or standard is “widely recognized.” Plus, the exception already requires that the technology and services be necessary and used predominantly to implement, maintain, or reestablish cybersecurity. Thus, donors and recipients are already subject to this requirement and are essentially making such a declaration by providing and accepting the technology</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>and services. In addition, the OIG may always bring an action against a physician who fails to use the technology and services predominantly to implement, maintain, or reestablish cybersecurity. Accordingly, the separate deeming provision is an unnecessary technical requirement.</p>
<p>2.1 ESTABLISHING MINIMUM CYBER HYGIENE PRACTICES FOR HEALTH CARE ORGANIZATIONS</p>	<ol style="list-style-type: none"> 1. How should Congress go about creating minimum cyber hygiene practices? Which federal agency should be responsible for development and implementation? What should be the incentives or penalties for compliance or noncompliance? 2. Regarding including these are part of a facility's Medicare Conditions of Participation – if this is not the preferred framework, why not? What makes cybersecurity—which we've learned has patient safety risks— different from other critical patient safety protections that are currently required? 	<p>Every organization or practice will face a different set of risk tolerances with respect to cyber hygiene and combatting cybersecurity risks. Creating minimum cyber hygiene practices should begin at a most basic level, especially if Congress is considering non-compliance penalties. According to a 2021 Healthcare Cybersecurity Survey conducted by the Healthcare Information and Management Systems Society (HIMSS), cybersecurity budget, followed by staff compliance with policies and procedures, legacy technology, and patch and vulnerability management were each a substantial and ongoing challenge. Congress may consider what should be included in minimum basic cybersecurity hygiene practices. Basic security controls, as reflected in the survey, could include antivirus/anti-malware, firewalls, email security gateway, encryption, patch and vulnerability management. Relatively few organizations are implementing a full complement of these basic controls but would benefit from these as the most foundational line of defense. We reiterate that small, solo, and rural practices will need additional financial resources to support their adoption of even basic controls.</p> <p>The AMA, however, strongly disagrees with making minimum cyber hygiene practices a condition of</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>Medicare participation. This type of policy step is a tremendous burden for physicians, especially small practices. This type of cybersecurity policy approach could inadvertently negatively impact patient access to care. For example, if cyber hygiene becomes a mandatory condition of participation, regardless of how basic these requirements may seem, it could result in physicians opting not to participate in the Medicare program. It would also further physician uncertainty in CMS program requirements which have already been shown to be overly burdensome, complex, and costly. With the nation contending with an ever-growing Medicare population, additional bureaucratic requirements that prompt physicians to no longer participate in this crucial government program—or further CMS program complexity—will negatively impact patients. Although we applaud the attempt to find ways to make cyber hygiene a more regular part of physician practices, the AMA urges federal policymakers to avoid alteration of any Medicare Conditions of Participation.</p>

<p>2.3 SOFTWARE BILL OF MATERIALS</p>	<ol style="list-style-type: none"> 1. Should a single agency or group be in charge of SBOM requirements? 2. Are health IT risks sufficiently grave or unique to warrant an accelerated or heightened SBOM approach from other commercial IT products? Should SBOM requirement be applied retroactively? 3. Should SBOM creation, publication, and sharing be mandatory or voluntary? 	<p>As evidenced by the release of this white paper and other similar documents and regulations from the executive branch, the AMA believes that the federal government is working to establish an effective national strategy to reduce cybersecurity vulnerabilities in the health care sector. Yet, more can be done through greater transparency including a Software Bill of Materials (SBOM), equitable distributing risk among the health care industry, and reframing the conversation to focus on positive incentives.</p> <p>Transparency</p> <p>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 information will position physicians to select EHR vendors and manufacturers that will support the practice’s cybersecurity needs.</p>
--	---	--

		<p>As a result, 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.</p> <p>As the 2017 U.S. Department of Health and Human Services (HHS) Health Care Industry Cybersecurity Task Force Report (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.” 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.</p> <p>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 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</p>
--	--	---

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		mitigation strategies when patches are not available.” The Task Force Report further notes that, “[t]o date, this practice has not been widely adopted.” The AMA urges Congress to ensure cybersecurity and/or SBOM legislation recognizes the supportive role SBOMs can play in physicians complying with HIPAA’s Security Rule.
2.4 STREAMLINING INFORMATION SHARING	3. If H-ISAC is the best entity for information sharing among health care organizations, could an incentive for smaller health sector entities be beneficial to the nation’s health care system? How should “smaller” health entities be defined? What would be an appropriate incentive for? Should H-ISAC be responsible for any incentive?	The AMA supports positive financial incentives for smaller practices, to help ensure bidirectional information sharing. Financial incentives are most effective when framed as a positive stimulus, as opposed to a penalty. Incentives implemented with the goal of enhancing information sharing by physicians should ensure that physicians receive a meaningful positive stimulus to support the necessary practical enhancements to bring about the desired improvements in information sharing. In practice, H-ISAC is predominantly used by larger providers, only.
2.5 FINANCIAL IMPLICATIONS FOR INCREASED CYBERSECURITY REQUIREMENTS	<ol style="list-style-type: none"> 1. How should Medicare payment policies be changed to ensure cybersecurity expenses are incorporated into practice expense and other formulas the same way other basic expenses are? 2. For “startup” grants, what should the eligibility criteria be for a grant program that provides small, rural, and independent providers with funding for cybersecurity? Who should administer such a grant program? What should be allowable uses of such funds? 	The AMA is conducting a significant practice expense collection effort in 2023/2024 to measure physician 2022 practice expense. As part of this effort, the AMA will ask practices to specify all information technology costs. The survey questionnaire asks the respondents to incorporate cybersecurity costs into their response. While preparing for this project, the AMA met with numerous physician practices. Many Chief Financial Officers and other financial experts articulated that these costs have become significant for physician practices. In light of the ongoing surveys related to practice expense that are expected to be conducted over the next two years, we urge Congress to work with the AMA as it relates to changes to Medicare payment policy and the incorporation of cybersecurity costs.

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>Once fully obtained, this data will prove useful for any future policy making.</p> <p>The AMA supports the proposal for startup grants to rural physicians. In addition, the AMA supports flexible eligibility criteria to ensure the maximum number of small, rural, and independent practices can qualify for these “startup grants.”</p>
3.1 CYBER EMERGENCY PREPAREDNESS	1. Should health care providers be required to train all staff members within the health care system to use alternate or legacy systems in the event of catastrophic failure to connected systems?	<p>The contemplated requirement is far outside the scope of the usual physician skill set, particularly with respect to small providers. Dissemination of the requisite resources should precede the implementation of mandates, or compliance will be unduly burdensome at best, and out of reach, at worst. Education and communication are vital to achieve success in any federal program requirement. CMS would, therefore, need to provide extensive outreach and support via the agency’s Medicare Learning Network® and the drafting and releasing of best practices. This effort should also be in close coordination with medical professionals and their associations.</p> <p>Regarding larger health systems, the Stark/Anti-Kickback statutory regime allows health systems to donate cybersecurity personnel to physician practices to help conduct training.</p>
3.3 DISASTER RELIEF PROGRAM	1. Is creating a new program specifically for cyber-related disasters preferred to simply making certain cybersecurity incidents eligible for FEMA disaster funds? Would states be required to provide non-	The AMA acknowledges that health care data interruptions are especially harmful due to potential physical harm to patients and calls for prosecution to the fullest extent of the law for perpetrators of ransomware and any other malware on independent

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
	<p>federal funding matches as they often do under FEMA disaster assistance?</p> <p>2. What should the criteria be to determine whether a cyber event experienced by a health care organization constitutes a “cyber disaster”? Who should determine this criteria? If the program is outside FEMA, who should administer?</p> <p>3. Would such a program conflict with existing cybersecurity insurance coverage?</p>	<p>physicians and their practices, health care organizations, or other medical entities involved in providing direct and indirect care to patients.</p> <p>The AMA supports federal legislation which provides for the prosecution of perpetrators of ransomware and any other malware on any and all health care entities, involved in direct and indirect patient care, to the fullest extent of the law. The AMA encourages health care facilities and integrated networks that are under threat of ransomware attacks to upgrade their cybersecurity and to back up data in a robust and timely fashion. Further, the security of protected health care information is appropriately considered as an integral part of national cybersecurity protection.</p> <p>Therefore, federal cybersecurity resources should be allocated to physician practices, hospitals, and health care entities sufficient to protect the security of the patients they serve. A significant portion of allocated funds should be earmarked for small physician practices. Disaster relief funds must be made readily available to small practices while any and all barriers to these resources must be removed.</p> <p>The AMA is essentially agnostic on whether the federal government should create a new cyber-related disaster program or permit affected entities to receive FEMA disaster funds. Providing ample financial resources to help physicians recover from cyber-attacks and ensuring that physicians, especially small practices, can easily qualify for these federal funds is the highest</p>

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		<p>priority for our members. During a cyber-attack, physician practices will suffer from diminished capabilities and the ability to apply for assistance should be streamlined and free of excessive bureaucratic red tape. Federal lawmakers should also exercise great caution in making any definition of “cyber-attack” too stringent in order to permit the maximum number of incidents to qualify for assistance. Although potentially small in scale, a cyber-attack that only impacts a solo practitioner or small practice can still be crippling for both the physician and patients. In a more connected and integrated health care space, small practices may often be an entry point for cyber attackers to access large health care systems. Federal disaster funds should also include technical support and knowledge workers that can assist practices in responding to and recovering from an attack to prevent more widescale cyber issues.</p>

<p>3.4 SAFE HARBOR/IMMUNITY IF HEALTH CARE ORGANIZATIONS IMPLEMENT ADEQUATE SECURITY MEASURES</p>	<ol style="list-style-type: none"> 1. Would health care organizations do more that would be beneficial to health care cybersecurity and patient safety, but for the fact that it opens them up to legal or regulatory liability? 2. Does indemnification of health care organizations present undue moral hazard, preventing them from adopting precautions and mitigations beyond a minimum threshold? 3. How can these provisions ensure patients have the continued right to access the justice system when they experience harm? 	<p>Protecting physicians, practices and other health care organizations from unnecessary or excessive legal or regulatory liability is always an important way to incentivize preferred behavior or activities. As a result, AMA supports indemnifying physicians and practices that implement and make good faith efforts to maintain proper cybersecurity protections from legal and regulatory liability. In fact, in 2015 the AMA House of Delegates adopted policy urging advocacy for indemnity or other liability protections for physicians whose electronic health record data and other electronic medical systems become the victim of security compromises (Policy D-315.977).</p> <p>As stated throughout this comment letter, policy efforts to expand cybersecurity protection are best viewed through the lens of a small physician practice that has limited resources. The time, expense, and expertise needed to implement proper cybersecurity protocols is already a daunting task for many practices. Layering the threat of additional legal or regulatory liability for compromises will only further exacerbate the reluctance of physician practices to pursue important cybersecurity protections.</p> <p>While sympathetic to policymaker’s concerns about moral hazard associated with indemnification, the AMA is confident that federal regulators still have ample tools at their disposal to pursue physicians and practices that exhibit gross or willful negligence of cybersecurity measures. Otherwise, the AMA urges policymakers to take the necessary steps to protect physicians and practices from excessive legal and regulatory liability in hopes of further promoting</p>
--	---	---

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
		adoption of greater cybersecurity protections within the health care industry.

Cybersecurity Policy Options Paper - Sections	Questions	AMA Response
3.5 CYBER INSURANCE	<ol style="list-style-type: none"> 1. Should Congress create a reinsurance program or otherwise regulate cyber insurance? 2. What can Congress do to facilitate information sharing between the intelligence community and insurers? 3. How can these provisions ensure patients have the continued right to access the justice system when they experience harm? 	<p>The nascent cyber insurance marketplace is characterized by numerous complicated policy questions. With the threat of cyber-attacks growing exponentially, the prospect of purchasing cyber insurance is likely an increasingly attractive business prospect for physician practices. Despite the absence of any official policy on this topic, the AMA urges federal policymakers to avoid mandates for purchasing cyber insurance, as this will have a disproportionate impact on smaller practices or play an excessive role in the regulation of the business (i.e., mandating policies provide a certain amount of coverage). A successful cyber insurance marketplace depends on the availability of ample policy choices at reasonable premiums. Excessive regulation or mandates to include certain concepts within specific cyber insurance policies could stifle the growth of this marketplace and lead to more expensive policy options that are not available to physician practices.</p> <p>While Congress should take a limited role in dictating the components of individual cyber insurance policies, a successful cyber insurance market will likely require a reinsurance program backed by the federal government. Major cybersecurity breaches within the health care sector, perhaps facilitated by foreign governments, could lead to massive financial losses for companies offering these policies. Therefore, federal reinsurance is a logical policy tool to help ensure the overarching stability of the cyber insurance marketplace.</p>