

July 1, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane
Washington, DC 20528-0380

Dear Director Easterly:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to offer our comments on the Cybersecurity and Infrastructure Security Agency's (CISA) notice of proposed rulemaking : Cyber Incident Reporting for Critical Infrastructure Act (CIRCI) Reporting Requirements. The AMA applauds CISA's ongoing leadership on cybersecurity policy and the agency's efforts to improve the safety, resilience, and security of our nation's critical infrastructure sectors, including the Health Care and Public Health Sector.

At a foundational level, the AMA supports cyber incident reporting for the largest entities within the Health Care and Public Health Sector. Cyber incident reporting is a meaningful piece of an entity's comprehensive cybersecurity plan. Cybersecurity needs to be prioritized and adequately addressed for several reasons, 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 greater risk. These aspects were identified by the AMA in 2017 and continue to be relevant to this day.¹

Our organization remains deeply concerned that health care providers and patients have been insufficiently prepared to meet the cybersecurity challenges of an increasingly digital health care system. We are 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, as well as a skilled workforce to secure sensitive patient information in the digital sphere. We see cyber incident reporting by covered entities under CIRCI as complementary to other cyber incident reporting that many health care organizations already provide to the U.S. Department of Health and Human Services (HHS) under the Breach Notification provisions of the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health (HITECH) Act, and to the Federal Trade Commission under Health Breach Notification Rule.

¹ <https://www.ama-assn.org/system/files/2018-10/cybersecurity-health-care-infographic.pdf>.

In addition, 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 our cybersecurity apparatus, especially with the increasing number of cyber-attacks focused on the health care sector.

Moreover, in the wake of the massive cyberattack on Change Healthcare, the AMA wants to ensure that attention is squarely focused on implementing solutions that improve health care's cybersecurity posture as a critical infrastructure sector. **The Change Healthcare cyberattack demonstrates the extreme interconnectedness within our critical sector, a significant dependency on one vendor, and the fragility of the system when that vendor suffers an attack and is nonfunctional.** The Change Healthcare attack offers a case study of the acute impact on patients, physicians, hospitals, pharmacies, labs, and countless additional health care professionals, providers, and entities across the country—particularly those small and independent physician practices that operate on a thin financial margin and did not have the resources to weather a storm of this magnitude. As a nation, we need to do better to protect our infrastructure, technologies, and systems from threat actors that seek to exploit our sensitive health care data, abuse the vulnerabilities of under-resourced populations, and promote widespread disruptions across the health care industry.

Overall, we want to ensure that cybersecurity initiatives in the health care sector focus on safeguarding protected health information and support equitable care delivery. Given the highly sensitive nature of an individual's personal information, **it is critical that cybersecurity programs support safeguards around patients' and other individuals' privacy interests and preserve the security and integrity of one's personal information.** The AMA sees cybersecurity as a patient safety issue, and physician practices prioritize cybersecurity to better serve their patients.

Our principal recommendations and feedback on CISA's policy proposals in the proposed regulation are as follows:

We agree that every individual provider of patient care should not be required to report covered cyber incidents and ransom payments

The AMA generally supports the criteria that CISA used to determine which entities in a critical infrastructure sector should be covered entities. With CISA considering the specific aspects of the three prongs of cybersecurity risk—consequence, threat, and vulnerability—to assess which entities will be deemed a “covered entity,” under the proposed Rule, **we agree that physician practices should not be considered a covered entity under this regulation.** As previously mentioned, physician practices are often small- to medium-sized entities that live financially on the margins. Many physicians are small business owners who cannot afford the expense of a full-time information technology (IT) professional and often must contract out for IT and/or cybersecurity services. Adding reporting requirements on practices would be an undue administrative burden on physicians, which would take time and resources away from direct patient care.

Ultimately, what physician practices need most is guidance, education, and resources to implement cybersecurity best practices. The AMA recommends that CISA and other government agencies in the cybersecurity space contemplate ways to **make cybersecurity best practices affordable, attainable, and approachable for physicians without extensive health IT knowledge, experience, or budgets.** This is particularly critical for practices in which physicians have primary responsibility for the health care cybersecurity role at their respective organizations.

The AMA supports positive financial incentives for physician practices to adopt cybersecurity best practices and 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 goals of enhancing information sharing as well as securing sensitive patient information by physicians should ensure that physicians receive a meaningful positive stimulus to support the necessary practical enhancements to bring about desired improvements. In addition, given the significant number of under-resourced small, solo, and rural physician practices, these small businesses will need additional financial resources beyond the incentive program dollars to support their adoption of even basic cybersecurity controls.

The AMA urges CISA to explicitly include health insurance companies and intermediaries (e.g., clearinghouses) as covered entities under this regulation

Within the Health Care and Public Health Sector, the proposed covered entities are large hospitals; critical access hospitals; manufacturers of essential medicines; and manufacturers of Class II and III medical devices. We support the inclusion of those entities and recommend the addition of sector-specific criteria for all health insurance companies and intermediaries.

As detailed in the proposed rule, CISA believes a sufficient number of health insurers already will be captured under the size-based criterion that applies across all critical infrastructure sectors. However, it is unclear if health insurer intermediaries and clearinghouses would necessarily meet the size-based criteria. **For that reason, CISA should specifically designate all health insurance companies, intermediaries, and clearinghouses as covered entities.**

As previously discussed, the Change Healthcare cyberattack clearly demonstrated the interconnectedness of the health care ecosystem and the importance of health insurance companies, intermediaries, and clearinghouses in maintaining public health and safety. Although Change Healthcare was not a well-known entity until recently, it is a health care giant. Even *before* UnitedHealth Group's (UHG) subsidiary Optum purchased Change Healthcare in 2022, the company facilitated over 15 billion health care transactions and approximately \$1.5 trillion in adjudicated claims—more than one-third of all U.S. health care expenditures annually.²

For many physicians, hospitals, and health insurance companies, Change Healthcare serves as a clearinghouse through which eligibility inquiries are received and responded to, claims are submitted and processed, and remittance is sent back to the physician or health care provider. For some payers, Change Healthcare even handles claims payment. Change Healthcare's importance as the "middleman" transmitting health care claims from physicians and hospitals to insurance companies in the United States cannot be overestimated. But that does not even come close to covering the extent of Change Healthcare's reach in the health care system.

Change Healthcare also plays a primary role in communicating prescriptions to pharmacies and determining pharmacy, insurance, and patient costs. It facilitates exchanges between physicians, hospitals, and labs—including the ordering of labs and the sending of results. Change Healthcare supports the exchange of information related to prior authorizations and other utilization management requirements. And it has products and services that reach into practice management systems and electronic health record

² Change Healthcare Annual Report (Form 10-K) for year ended Dec. 31, 2020, available at https://ir.changehealthcare.com/node/7326/html#tx904010_8.

(EHR) systems for dozens of other practice management, clinical, and revenue cycle purposes. When Change Healthcare turned off its systems on February 21 upon news of the cyberattack, the U.S. health care system more or less came to a screeching halt.

For nearly three months, the Change Healthcare systems and products that many physicians and hospitals depended upon were not up and running, at least not completely, and physician practices had to try to function without all the Change Healthcare services on which they depended. To a certain extent, the impact of this cyberattack is still being felt today and affecting patient care as well as the functioning of physician practices. Moreover, the true scale of the cyberattack has still not been disclosed, including how many patients have had their personal health information compromised. For context, in testimony before the Senate Finance Committee on May 1, 2024, Andrew Witty—Chief Executive Officer of UHG—stated that the cyberattack could impact a “substantial proportion of people in America.”³

The proposed rule presents the factors that Congress expected CISA to use to assess the inclusion of certain entities as covered entities. These factors include the consequences that disruption or compromise of an entity could cause to public health and safety; the likelihood that an entity may be targeted by a malicious cyber actor; and the extent to which damage, disruption, or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure. **The Change Healthcare cyberattack encompasses all these factors and makes the case for including specific criteria focused on health insurance companies, intermediaries, and clearinghouses in CIRCIA’s Health Care and Public Health Sector.**

Provide more clarity on CISA actions after submission of covered Cyber Incident and Ransom Payment Reports.

The AMA supports the use of a web-based CIRCIA Incident Reporting Form, and the abundant details provided on the requirements for covered entities related to how to submit reports, the format of the reports, the proposed content to be included, and the extent of liability protections. However, **inadequate information is conveyed about how CISA plans to use the information that it collects through these reports and what outputs and conclusions will be returned to the covered entities submitting a report, as well as to the broader community of stakeholders.** Much like the details provided about the reports submitted to CISA, it is important to describe the cyber threat information that will be shared with submitters and other entities in their critical infrastructure sector.

As described in the Proposed Rule, CIRCIA requires CISA to provide timely, actionable, and anonymized reports of cyber incident campaigns and trends as well as contextual information, cyber threat indicators, and defensive measures. **CISA needs to provide more specifics around the information that it plans to distribute about what it learns from the cyber incident and ransom payment reports.** If CISA wants to build sustainable support for CIRCIA-related reporting, it must demonstrate that the investment of time and resources in submitting a report will yield benefits and knowledge for submitters. It is also imperative that CISA focus on returning actionable information to covered entities and the community-at-large.

³ <https://www.finance.senate.gov/hearings/hacking-americas-health-care-assessing-the-change-healthcare-cyber-attack-and-whats-next>.

Ultimately, CISA should plan to share information collected from reports with the covered entities that submit them, other covered entities within that covered entity's critical infrastructure sector, and, if broadly applicable, all covered entities in each critical infrastructure sector, as well as the wider community. There should also be an educational component to the information that is shared broadly with stakeholders so that they know what steps to take to mitigate the threat, even if they are not cybersecurity experts or well-versed in technology frameworks.

For example, even with physician practices not being designated as CIRCIA covered entities, we expect that some threat information may be applicable to them based on their physical location, affiliations/partnerships, vendors, or systems. However, as practices likely do not have extensive health IT knowledge, experience, or budgets, **information shared with them must be delivered in a format that is easily consumable and actionable to them.** While physician practices may not have the number of attack surfaces that other covered entities have, if cyber threat information is available that could impact their practice, or the safety of their patients, it should be shared with them with actionable information on what steps to take to mitigate each threat.

CISA should also investigate leveraging the 23 sector-based Information Sharing and Analysis Centers and other trusted industry not-for-profit organizations to communicate the threat information collected back to community members. These organizations would better know the individual members within each of their sectors and be familiar with the different aptitudes and knowledge bases to clearly communicate threat information and actionable next steps in a format that they can use.

Create new regional extension center program to help educate small entities across all critical infrastructure sectors on cybersecurity best practices.

The HITECH Act of 2009 created the Regional Extension Center (REC) program⁴ that the HHS Office of the National Coordinator (ONC) used to provide on-the-ground technical assistance for individual and small physician practices and other medical practices lacking resources to implement and maintain EHRs. The focus was on assisting those providers in local communities that serve those who lack adequate health insurance coverage or medical care. **ONC's REC Program can serve as a model for CISA to consider helping small and under-resourced entities in all critical infrastructure sectors that need assistance in implementing cybersecurity best practices.**

For the Health Care and Public Health Sector, we envision that a CISA-led REC Program could help the small- to medium-sized physician practices that operate on a thin financial margin and do not have the resources to hire a cybersecurity specialist yet are concerned about securing their network and protecting their patient's personal health information.

Such a program would help address the shortage of available health IT and cybersecurity professionals and the lack of cybersecurity expertise in many physician practices. **RECs could also help small physician practices tackle cybersecurity issues as they arise and respond to information that CISA shares with the community about vulnerabilities that surface from CIRCIA Cyber Incident and Ransom Payment Reports.**

As part of this broader effort around cyber incident reporting, the AMA encourages CISA to consider implementing a REC-like program to assist small- to medium-sized physician practices with their cybersecurity needs and also support small entities that are part of other critical infrastructure sectors.

⁴ <https://www.healthit.gov/topic/regional-extension-centers-recs>.

The Honorable Jen Easterly

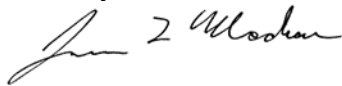
July 1, 2024

Page 6

The AMA believes that this proposed rule will improve the safety, resilience, and security of our nation's critical infrastructure sectors, including the Health Care and Public Health Sector. **The AMA applauds CISA's ongoing leadership on cybersecurity policy and the agency's attention to the cybersecurity needs of small- to medium-sized physician practices that live financially on the margins.**

We look forward to working with CISA to fulfill these goals and ensure that physician practices can prioritize implementing cybersecurity best practices in order to better serve their patients and protect their personal health information. Thank you for the opportunity to provide comments on this proposal. If you have any questions, please do not hesitate to contact Margaret Garikes, Vice President of Federal Affairs, at margaret.garikes@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