



July 1, 2024

The Honorable Alejandro Mayorkas
Secretary
Department of Homeland Security
2707 Martin Luther King Jr. Ave. SE
Washington, D.C. 20528

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Rd.
Arlington, VA 20598-0630

Re: Docket No. CISA–2022–0010; Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements

Dear Secretary Mayorkas and Director Easterly:

On behalf of the American Academy of Family Physicians (AAFP), which represents more than 130,000 family physicians and medical students across the country, I write to provide comments on the *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements* proposed rule from the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Homeland Security (DHS), as requested in the April 4, 2024, [Federal Register](#). The AAFP appreciates DHS and CISA’s attention and interest in this important issue that is a significant concern for primary care physicians and practices. As detailed further below and in addition to other recommendations, **the AAFP urges CISA to:**

- **Work with Congress and federal agencies to align the terms and definitions used in this rulemaking with other relevant regulations and laws.**
- **Not hold Critical Access Hospitals (CAHs) to the same reporting requirements as large hospitals without offering additional education and implementation support.**
- **Develop and finalize specific applicability criteria for health IT vendors and health insurance companies, thereby appropriately acknowledging their potentially outsized roles in the health care sector’s critical infrastructure.**
- **Not expand applicability criteria to additional physicians and practices beyond those outlined in this proposal.**
- **Work with HHS to reach an appropriate information sharing agreement before these regulations are finalized so physicians and hospitals can avoid unnecessary, duplicative, burdensome reporting requirements.**

The migration to digital health and electronic storage of patient health data has improved patients’ ability to access their health information. The AAFP has long [supported](#) policies that guarantee the appropriate security of protected health information, while also working to improve patients’ access to their data and increase capabilities to share patients’ health information across the care team. We are strongly [supportive](#) of making data reliably interoperable while maintaining patient confidentiality and the fundamental right to privacy. A confidential relationship between patient and physician is essential for the free flow of information that is necessary for sound medical care, and confidentiality of patient health data should continue to be a priority outside of the patient-physician relationship.

However, the rapid move to this electronic era of health care has unavoidably introduced the risk of

STRONG MEDICINE FOR AMERICA

President
Steven Furr, MD
Jackson, AL

President-elect
Jen Brull, MD
Fort Collins, CO

Board Chair
Tochi Iroku-Malize, MD
Islip, NY

Directors
Gail Guerrero-Tucker, MD, *Thatcher, AZ*
Sarah Nosal, MD, *New York, NY*
Karen Smith, MD, *Raeford, NC*
Kisha Davis, MD, MPH, *North Potomac, MD*
Jay Lee, MD, MPH, *Costa Mesa, CA*
Teresa Lovins, MD, *Columbus, IN*

Sarah Sams, MD, *Dublin, OH*
Brent Smith, MD, *Cleveland, MS*
Jefferey Zavala, MD, *Billings, MT*
Matthew Adkins, DO (New Physician Member), *Columbus, OH*
Janet Nwaukoni, DO (Resident Member), *Grayslake, IL*
Taree Chadwick (Student Member), *Reno, NV*

Speaker
Russell Kohl, MD
Stilwell, KS

Vice Speaker
Daron Gersch, MD
Avon, MN

Executive Vice President
R. Shawn Martin
Leawood, KS

cyberattacks for all health care organizations. More than 45 million people were affected by cybersecurity attacks on health care professionals in 2021,ⁱ and it's estimated that one-third of Americans had their health data breached during the recent Change Healthcare cyberattack.ⁱⁱ The AAFP educates and encourages our members to work with their electronic health record (EHR) vendors, medical device vendors, and other partners to adopt data privacy and security practices, including cybersecurity protections. While privacy and security of patient health data is a priority for physician practices, not all of them have the resources, financial capacity, or technical knowledge needed to properly establish and implement best practices in cybersecurity. Many hospitals struggle to maintain appropriate resources, let alone small health care organizations, despite hackers likely having the same access to both. In any health care setting, health information technology (IT) vendors must be held accountable both to ensure cybersecurity protections and to manage the consequences from any data breach or cyberattack on patient health and practice operations.

Definitions

CISA proposes to define “cyber incident,” “covered cyber incident,” and “substantial cyber incident” in this rule, all of which are definitions the AAFP supports. Additionally, we understand that CISA is utilizing a meaning of “covered entity” that is defined in statute (6 U.S.C. 681(4)) and appreciate the agency’s efforts in this proposed rule to further clarify the criteria for covered entities as is statutorily required. However, we [remain concerned](#) that federal agencies use a variety of definitions for key terms, such as “covered entity.” Disparate definitions for the same terms across different regulations can create confusion and administrative burdens for physicians working to ensure they are in compliance. Given the importance of the Health Insurance Portability and Accountability Act’s (HIPAA) definition of “covered entity” and how firmly established its meaning is within the health care system, we are concerned this differing definition will cause significant confusion. **The AAFP urges CISA to work with Congress and other federal agencies to align the terms and definitions used in rulemaking with other relevant regulations and laws.** Additionally, we encourage the agency to undertake a substantial education campaign to ensure that impacted health care facilities and stakeholders understand these contrasting definitions of “covered entity.”

Applicability

CISA proposes three criteria for required CIRCIA reporting for covered entities under the “Healthcare and Public Health Sector” section of this rule: 1) any entity that owns or operates either a hospital with 100 or more beds or a critical access hospital; 2) manufacturers of drugs listed in Appendix A of HHS’ *Essential Medicines Supply Chain and Manufacturing Resilience Assessment* report; and 3) manufacturers of FDA-classified Class II and III devices. Additionally, any owner or operator of a health care facility that exceeds the Small Business Administration’s (SBA) [Table of Size Standards](#) (determined by annual revenue) would also be required to report a cyber incident to CISA.

The AAFP strongly agrees with CISA that health care facilities and the public health system are key to maintaining the health of the nation and global health security, and we appreciate the proposal to utilize a size-based criterion built on SBA small business standards. We agree with the agency that larger hospitals have a greater likelihood of experiencing significant impacts if they fall victim to a covered cyber incident and are more likely to have the necessary cyber expertise to identify, respond to, and report a cyber incident. CISA’s proposed standards would also capture other large entities that play a critical role in the operations of the health care system, such as large

claims clearinghouses. Focusing reporting obligations on large entities would avoid placing a disproportionate burden on smaller practices, which are already facing operational challenges and administrative burdens with limited resources.

The AAFP is concerned by CISA's proposal to hold large hospitals (100+ beds) and critical access hospitals (CAHs) to the same standards and reporting requirements. While we agree with CISA that CAHs are often the only source of emergency health care for individuals living in rural areas, the proposed rule does not discuss or acknowledge the vast resource differences – financial, technological, and staffing – between large hospitals and CAHs. Given that the CAH designation was created specifically to [reduce the financial vulnerability](#) of rural hospitals and that CAHs are less profitable than non-CAHs,ⁱⁱⁱ **the AAFP urges CISA to reconsider holding CAHs to the same reporting requirements as large hospitals without offering them additional education and implementation support.**

While the AAFP understands CISA's reasons for proposing to not include specific criteria for health insurance companies and health IT vendors, **we urge the agency to reconsider and to develop specific criteria for health IT vendors and health insurance companies because of their potential to have an outsized impact on the health care sector if targeted in a cyberattack.** Due to the same potential for outsized negative impacts on the health care system if attacked, the AAFP also believes CISA should develop specific criteria for insurer-owned third-party provider service networks—especially given the technology platforms provided to and used by such insurer-owned provider networks are often extensively connected to EHRs, health information exchanges, registries, and more. Private insurance companies and health IT providers are often underregulated, while physicians and practices continue to accumulate administratively burdensome reporting requirements through regulation. Though it is likely that most private payers would meet the size criteria proposed here, not all would, and the loss of a payer would significantly disrupt care for patients using that company. We believe payers are just as much part of the health care system's critical infrastructure as hospitals are and should be treated accordingly.

Additionally, it seems disingenuous for CISA to justify not including criteria for the health IT community due to their reporting obligations under the HIPAA Health Breach Notification Rule and Health Information Technology for Economic and Clinical Health Act (HITECH Act) Health Breach Notification Rule, considering health systems are also obligated to report under both of those rules and have specific criteria proposed in this rule. While health IT software can be developed and sold using a relatively small staff, it could also impact an outsized number of health care practitioners if cybersecurity vulnerabilities in those products were exploited. For example, the two largest EHR vendors in the country are used by almost 60% of the nation's hospitals.^{iv} If a cyberattack took one of those systems offline, it would impact at least one in five U.S. hospitals. Due to the outsized risk posed, the AAFP believes that all health IT vendors, regardless of size, should be covered by this rule.

The AAFP strongly believes that additional health care practices engaged in direct patient care should not be included in this regulation. While large hospitals with significant administrative and IT staff and substantial financial reserves may be equipped to fulfill the proposed requirements outlined here on the timeline discussed, small physician-owned practices are in an entirely different situation—particularly primary care practices that frequently operate on razor thin margins in the best of times. **We support CAHs remaining in this proposal only if CISA offers a robust foundation of**

education and implementation support, and we urge the agency not to expand the applicability criteria to additional physicians and practices.

Required Reporting on Covered Cyber Incidents and Ransom Payments

CISA proposes four circumstances that would require covered entities to submit a report to the agency, which we support. However, the AAFP does not support the agency's proposal to require each covered entity involved in a single cyber incident to submit a report to CISA, and as outlined above, we believe health insurance companies and health IT vendors should be explicitly included in the final rule as covered entities. Given the recent cyberattack at Change Healthcare and the months of related challenges AAFP members have faced – including administratively burdensome workarounds, implementing manual mechanisms in cases where workarounds failed, and, in many cases, leaning on outside sources of financial assistance or forgoing their own compensation in order to maintain adequate operations – it is crucial for CISA to consider how this proposed rule would have impacted the health care sector had it been in place when the attack occurred. Covered entities would have been asked to calculate the costs on their business at a time of extreme stress and while already overburdened from trying to restore or recreate business processes. While the AAFP understands that one goal of this proposed rule is to be able to determine how many organizations are impacted by individual cyber incidents and analyze related data, we question whether that proposed added burden is necessary to meet the intent of the law and if the information gained would be worth the effort expended. **When a single entity such as Change Healthcare is at fault for a covered cyber incident, reporting that incident and its related consequences to federal agencies should be the singular responsibility of the originating entity, not other impacted organizations.**

Exceptions to Required Reporting on Covered Cyber Incidents and Ransom Payments

CISA proposes four exceptions in which a covered entity would not have to submit a report regarding a qualifying cyber incident. The second proposed exception outlines that an entity can be exempt of these proposed reporting requirements if legally required to submit “substantially similar information within a substantially similar timeframe” to a different federal agency with whom CISA has an information sharing agreement. **While the AAFP acknowledges that HIPAA reporting requirements operate under a significantly longer timeframe than the 72 hours proposed in this rule, we strongly urge CISA to collaborate with HHS on ways to establish an information sharing agreement and minimize duplicative reporting for health care facilities.** Something as simple as a checkbox on CISA's incident form that reads, “Would you also like to notify HHS of a HIPAA violation?” and vice versa for CISA on HHS' HIPAA violation form, could be extremely effective in minimizing reporting burdens within the health care sector. This would allow any reporting entity to avoid a tremendous amount of administrative burden by not having to report the incident twice. **To prevent physicians and hospitals from being faced with unnecessary, duplicative, burdensome reporting requirements, the AAFP strongly urges CISA to work with HHS to reach an appropriate information sharing agreement before these regulations are finalized or go into effect.**

Data and Records Preservation Requirements

CISA proposes any covered entity that submits a CIRCIA report must preserve data relevant to the reported cyber incident. The data proposed to be preserved includes indicators of compromise; communications between the covered entity and the attacker; relevant log entries, memory captures, and forensic images; data related to any ransom payments made; and any reports produced or procured by the covered entity related to the cyberattack. The agency also specifies that even if an impacted organization used a third party to submit a CIRCIA report on its behalf, the covered entity would be responsible for preserving the relevant information after the fact. While the AAFP does not object to the types of data an organization would need to preserve if this is finalized as proposed, **we do encourage CISA to utilize the outreach and education campaign required by CIRCIA so that every likely covered entity can understand its responsibility in properly preserving data, particularly for cases in which a third party submits the CIRCIA report.** Additionally, the AAFP appreciates the proposed data preservation flexibilities outlined for covered entities and agrees with CISA that flexibilities are necessary to provide organizations the ability to preserve data in a convenient, cost-effective manner.

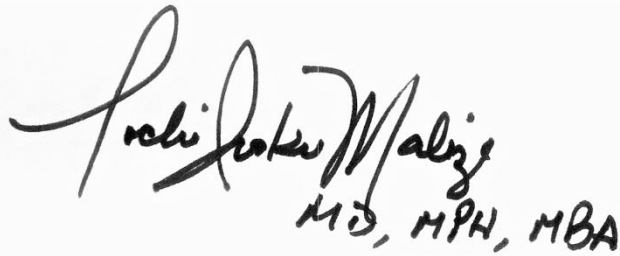
Enforcement

CISA outlines a proposed enforcement process in which the Director may issue a request for information (RFI) from any covered entity the Director believes has failed to submit a CIRCIA report in accordance with regulatory requirements. If the covered entity does not provide an adequate response to the RFI within 72 hours, the Director may then issue a subpoena. The AAFP understands that, by statute, the Director may issue a subpoena if an RFI has not been answered within 72 hours. **However, the AAFP encourages CISA and the Director to utilize the flexibilities also outlined in statute – such as issuing a second RFI if the first goes unanswered – and to use subpoena power sparingly.** In the immediate aftermath of a cyberattack, health care facilities are dealing with huge disruptions to clinical workflows and administrative processes, all while prioritizing patient safety. The AAFP agrees that CISA being informed of such an incident in a timely manner is important for the safety of the country's critical infrastructure, but we urge the agency to consider how overwhelming and chaotic the first 72 hours after a cyberattack can be. **Caring for patients will always be our members' first priority, and we hope CISA will demonstrate understanding and utilize available flexibilities when health care sector cyber incidents occur.**

Conclusion

Thank you for the opportunity to offer feedback on the policy proposals included in this proposed rule. We look forward to partnering with CISA, DHS, and other federal stakeholders to strengthen cybersecurity in the health care sector in an attainable and sustainable way for primary care physician practices to protect patient health data. Please contact Mandi Neff, Regulatory and Policy Strategist, at mneff2@aafp.org with any questions or concerns.

Sincerely,



Tochi Iroku-Malize
MD, MPH, MBA

Tochi Iroku-Malize, MD, MPH, MBA, FAAFP
American Academy of Family Physicians, Board Chair

ⁱ Milstein J. 2022. Critical Insight Finds 35 Percent Increase in Attacks on Health Plans in 2021 End of Year Healthcare Data Breach Report. Critical Insight. <https://www.criticalinsight.com/resources/news/article/criticalinsight-finds-35-percent-increase-in-attacks-onhealth-plans-in-2021-end-of-year-healthcare-data-breach-report>

ⁱⁱ <https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack>

ⁱⁱⁱ Pai DR, Dissanayake CK, Anna AM. A comparison of critical access hospitals and other rural acute care hospitals in Pennsylvania. *J Rural Health*. 2023; 39: 719–727. <https://doi.org/10.1111/jrh.12755>

^{iv} <https://www.definitivehc.com/blog/most-common-inpatient-ehr-systems>