July 3, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
1110 North Glebe Road
Arlington, VA 20598-0630

Re: Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements, 89 FR 23644

Dear Director Easterly:

On behalf of our member medical group practices, the Medical Group Management Association (MGMA) is pleased to provide the following comments in response to the Cybersecurity and Infrastructure Security Agency (CISA) proposed cyber incident reporting requirements under the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA). CISA proposes to institute reporting requirements for significant cyber events for critical infrastructure sectors including healthcare. We appreciate the agency's attention to this issue and ongoing work to enhance cybersecurity capabilities within the healthcare industry.

With a membership of more than 60,000 medical practice administrators, executives, and leaders, MGMA represents more than 15,000 medical group practices ranging from small private medical practices to large national health systems, representing more than 350,000 physicians. MGMA's diverse membership uniquely situates us to offer the following policy recommendations.

As harmful cyberattacks continue to impact a multitude of sectors in this country, we understand CISA's need for timely information related to attacks to mitigate threats, increase risk awareness, and support national security. CIRCIA was enacted to balance gathering cyber incident reporting quickly, while not imposing burdensome reporting requirements on organizations suffering from a cyberattack. While we appreciate CISA's work on this issue and the opportunity to offer feedback, we have considerable concerns about instituting burdensome, confusing, and duplicative reporting requirements that may impact medical groups' ability operate effectively, especially in the midst of a significant cyber incident.

MGMA offers the following recommendations to improve cyber incident reporting and minimize additional costly reporting burdens.

Key Recommendations

- **Harmonize CISA's proposal with other federal agency reporting requirements to allow for seamless and straightforward cyber incident reporting which removes unnecessary and duplicative reporting requirements.** CISA should reduce the burden by refining the required data that must be reported and allowing flexibility for covered entities.

- **Substantially increase the size-based threshold for medical groups** and avoid expanding reporting requirements to those physician practices not currently covered in the proposal.
- **Clarify ambiguous definitions and criteria** and align terminology with the Department of Health and Human Services (HHS) and other agencies.
- **Provide financial support to medical groups** to bolster cyber reporting and defenses, as well as necessary guidance, training, and resources.
- **Institute collaborative policies instead of overly punitive penalties** to further CISA's goals while also working to prevent cyberattacks in the future.

Harmonize CISA's Proposal with Other Federal Reporting Requirements and Reduce Reporting Burden

The proposed rule includes reporting requirements that would mandate covered entities disclose specific information related to a significant cyber incident and impacted information systems such as "technical details and physician locations of such networks, devices, and/or information systems." Covered entities would be responsible for proving information related to their security defenses, detection methods that were used to discover the attack, and more. CISA proposes to use a web-based form to potentially facilitate the transfer of this information.

The agency would implement a 72-hour time limit for covered entities to report on a significant cyber incident, and a 24-hour time limit to report a ransomware payment. While we appreciate the need for timely data, medical groups continue to provide high-quality patient care even when experiencing criminal cyberattacks against them. Given their commitment to treating their communities, there need to be flexibilities instituted given the complicated task of assessing a significant cyber incident and reporting to CISA so shortly after it has occurred.

Medical groups are already subject to various reporting requirements from HHS under HIPAA. Instead of implementing the duplicative reporting requirements in this proposed rule, we strongly urge CISA to work closely with HHS to avoid layering complex requirements on one another. While there are different timeframes for HIPAA Breach Notification Rule, **the agencies should work together to seamlessly incorporate data that will already be reported to not only promote collaboration but ease the burden of reporting on the same incident multiple times in multiple different formats.**

The last thing we want to do is enshrine in regulation a competing priority that takes resources away from patient care, especially at such a vulnerable time. The proposed reporting requirements are too extensive as much of the information needed may not be available. **CISA should reduce the required reporting elements and work with the industry to simplify requirements and understand the landscape of cyber threats before finalizing any regulations.**

The recent attack on Change Healthcare crippled much of this nation's health system given Change's wide reach in the industry, with medical groups suffering substantial harm.[1] A multitude of covered entities would likely be responsible for submitting reports to CISA as result of a similar cyberattack on the originating covered entity. **CISA should include language that allows for a singular report from the originating covered entity that has experienced a significant cyber event impacting many other covered entities.**

[1] MGMA, Letter to HHS on Change Healthcare cybersecurity attack, Feb. 28, 2024.

Lastly, given that sensitive information will be shared under this proposed rule, it is essential that all facets of reporting and storage of this data be done with the upmost protection against attempted hacks or improper disclosures. It is imperative to not create a single source of confidential information related to numerous critically important institutions without robust security measures.

Scope of the Proposed Rule

CISA proposes to include a size-based threshold to determine what entities are responsible for the cyber reporting requirements. Covered entities under the proposal are entities within a critical infrastructure sector that "exceed the U.S. Small Business Administration's (SBA) small business size standard based on either number of employees or annual revenue, depending on the industry." SBA size standards vary by industry and are specified by the North American Industry Classification System Code (NAICS) under 13 CFR part 121. The threshold for physician offices (NAICIS Code 621111) is $16.0 million in receipts, while other specialists have a threshold of as little as $9.0 million.[2]

An entity in a critical infrastructure sector will need to determine which NAICS code should apply to the entity and whether the entity meets the applicable receipts-based threshold or employee-based threshold. The Small Business Size Regulations provide requirements for how to determine if an entity qualifies as a small business. CISA is proposing that an entity should follow the instructions in 13 CFR part 121, or any successor, when determining whether it meets the size threshold.

While we appreciate CISA's inclusion of a size-based threshold to avoid instituting considerable reporting requirements for small medical groups who are already dealing with a litany of issues trying to keep their doors open — cuts to Medicare reimbursement, staffing shortages, rising costs, and more — MGMA harbors concerns that utilizing the current SBA small business standard will still unduly impact smaller physician offices reporting revenue of as low as $9.0 million per year. These groups are experiencing the same staffing shortages and escalating costs as even smaller practices, and while the effects may not be as pronounced, they are still severe.

CISA also proposes to establish sector-based criteria specific to healthcare — hospitals with 100+ beds and Critical Access Hospitals (CAHs) would fall under this proposed rule's purview and be subject to reporting. The parameters of the sector-based proposal further exemplify the proposal rule's incongruency related to smaller practices/organizations being required to report:

> "Many different types of entities provide direct care to patients, such as hospitals, clinics, urgent care facilities, medical offices, surgical centers, rehabilitation centers, nursing homes, and hospices. The size of the facilities, the number of patients cared for daily, and the types of services provided can vary dramatically across these entities. While all of these various types of entities contribute to the nation's public health and well-being, CISA does not believe it is prudent or cost-effective to require covered cyber incident and ransom payment reporting from every individual provider of patient care. Rather, CISA is proposing to focus on hospitals, as they routinely provide the most critical care of these various types of entities, and patients and communities rely on them to remain operational, including in the face of cyber incidents affecting their devices, systems, and networks to keep them functioning."

MGMA appreciates CISA acknowledging that it would not be prudent to institute additional reporting burden broadly throughout the healthcare sector. This logic applies to not only hospitals and CAHs (who

[2]U.S. Small Business Administration, Table of Size Standards, March 17, 2023.

have their own resource constraints), but also medical groups. **Should the agency not significantly simplify and reduce reporting burden, we urge CISA to substantially increase the threshold to physician practices from the currently proposed SBA threshold,** as this would more accurately capture medical groups that are more likely to incorporate these proposed requirements in a way that would not disrepute operations and potentially leave them open to government sanctions. **We oppose any expansion of the current scope of the rule to include additional physician practices.**

It is imperative to include a unified reporting regime that does not leave reporting gaps where CISA would not receive pertinent information. The proposed rule discusses health information technology (IT) vendors being subject to reporting requirements under HIPAA and the HITECH Act. Medical groups are subject to these requirements as well, and while some health IT vendors and health insurance companies may be covered under sector-specific or the size-based criteria, it is important to acknowledge their importance and how interconnected they are in the healthcare industry. Instituting comprehensive reporting polices that account for health IT vendors and health insurance companies is essential so that there are no gaps, and so the onus for reporting cyber incidents in other organizations does not fall to medical groups.

Clarification of Definitions

The proposed rule defines a "substantial cyber event" as any of the following:

- (a) a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
- (b) a serious impact on the safety and resiliency of a covered entity's operational systems and processes;
- (c) a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
- or (d) unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.

CISA offers examples of both what would be and wouldn't be considered a significant cyber event, but given the breadth of scenarios that may require reporting by covered entities, we ask for further clarity on the topic. The listed criterion for reporting encompasses numerous situations that may require reporting for minor incidents of no real value to CISA. The agency should avoid overly broad reporting requirements and refine what constitutes a "significant cyber event" to focus on those critical events that will truly provide helpful information to the agency.

Further, the proposed rule includes definitions of "covered cyber incident" and additional terms related to cyber events; these similar but separately defined terms will add uncertainty for physician practices attempting to comply. **We recommend CISA tighten these definitions to focus on truly significant cyber incidents and avoid superfluous and likely unhelpful reporting. The agency should work closely with HHS and other federal agencies to institute definitions that are aligned with ones already in statute and regulation.** Unifying and properly tailoring the definitions in the proposal is critical so the agency does not unduly burden medical groups with vague and confusing reporting requirements.

Supplemental Reporting and Data Retention Requirements

The proposed rule acknowledges that all the facts may not be known immediately following a cyber incident, and requires the prompt filling of supplemental reports when "substantial new or different information" becomes available. CISA further proposes that covered entities that submit a CIRCIA report must preserve specific data (log entries, forensic images, etc.) relevant to the cyber incident for two years. Should a covered entity use a third-party organization to submit its report, the covered entity would still be tasked with maintaining relevant data after the fact.

CISA should clarify and reduce the amount of information needed in a supplemental report and its data retention requirements so as to not institute an overly complex and costly compliance regime once the cyber incident is over. Covered data may not typically be stored for the years required by the proposed rule; capturing, sharing, and retaining the necessary data will add a significant cost to medical groups. CISA should shorten the timeframe required for covered entities to retain data and streamline the required information. This is necessary to avoid instituting unnecessary financial costs for medical groups.

Support and Resources for Providers

The proposed rule estimates that the cost of compliance to the industry will be $1.4 billion — this is a substantial financial burden placed on medical groups already struggling under numerous financial pressures. The Biden Administration acknowledged the significant costs associated with cybersecurity by including $500 million in its proposed 2025 budget for hospitals to bolster cyber defenses.[3]

Medical groups need a similar infusion to not only combat sophisticated attacks from bad actors, but to ensure the right infrastructure, staffing, and procedures are implemented to comply with additional reporting requirements proposed here. Adequate education and resources (training, fact sheets, webinars, etc.) will be needed to help medical groups understand and comply with any new reporting requirements CISA may finalize.

Enforcement

The proposal includes an enforcement regime that utilizes requests for information (RFIs) should CISA not receive a mandated report. The agency can ultimately utilize subpoenas and cases can be referred to the Attorney General to bring a civil action and potential contempt of court actions, among other penalties.

We urge the agency to incorporate commonsense policies to allow covered entities additional time to respond to an RFI given the myriad legitimate circumstances that may delay their ability to properly respond, as well as include an avenue for covered entities to specify why they are unable to comply without leading to further scrutiny and potential sanctions. Adding new penalties to victims of cybercrimes would be overly punitive and counterproductive to the intention of CIRCIA. **MGMA recommends CISA revise their enforcement approach so that it promotes collaboration between the agency and medical groups without adding penalties that would amplify the damage done by criminals perpetrating cyberattacks.**

Conclusion

MGMA thanks CISA for its leadership in protecting this nation's medical groups from malicious cyberattacks. We urge the agency to incorporate the above recommendations and avoid instituting

[3] Department of Health and Human Services, Fiscal Year 2025 Budget in Brief.

onerous reporting requirements for physician practices operating under substantial financial and resource constraints while dealing with a significant cyber incident. If you have any questions, please contact James Haynes, associate director of government affairs, at jhaynes@mgma.org or 202-293-3450.

Sincerely,

/s/

Anders Gilberg
Senior Vice President, Government Affairs