AMERICA'S ESSENTIAL HOSPITALS

July 2, 2024

Alejandro Mayorkas
Secretary
Department of Homeland Security
2707 Martin Luther King Jr Ave. SE
Washington, DC 20528-0525

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

**Ref: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Proposed Rule [Docket No. CISA-2022-0010]**

Dear Secretary Mayorkas and Director Easterly:

Thank you for the opportunity to comment on the above-captioned request for information. America's Essential Hospitals welcomes the Cybersecurity and Infrastructure Security Agency's (CISA's) work to fill gaps in the current cybersecurity reporting landscape and enhance the capacity of the U.S. government to support organizations as they address the fallout of cyberattacks.

America's Essential Hospitals is the leading association and champion for hospitals dedicated to equitable, high-quality care for all, including those who face social and financial barriers to care. Since 1981, America's Essential Hospitals has advanced policies and programs that promote health, health care access, and equity. We support our more than 300 members with advocacy, policy development, research, education, and leadership development. Our members provide a disproportionate share of the nation's uncompensated care (UC), and three-quarters of their patients are uninsured or covered by Medicare or Medicaid. Essential hospitals provide state-of-the-art, patient-centered care while operating on margins less than one-quarter that of other hospitals.[1]

Essential hospitals are dedicated to enhancing cybersecurity to protect patient data and improve health care delivery. The unprecedented cyberattack on Change Healthcare acutely affected our members, which had to divert limited staff time and resources to mitigate the

[1] Taylor J, Ramiah K, Greig M, et al. *Essential Data: Our Hospitals, Our Patients—Results of America's Essential Hospitals 2021 Annual Member Characteristics Survey*. America's Essential Hospitals. October 2023. essentialdata.info. Accessed May 29, 2024.


AMERICA'S ESSENTIAL HOSPITALS
401 Ninth St NW Ste 900
Washington DC 20004
t: 202 585 0100
f: 202 585 0101
e: contact@essentialhospitals.org

fallout of this attack and return to standard operations. Because essential hospitals have more limited resources than other hospitals because of their unique role in their communities, responding to this cyberattack was particularly challenging for our members.

Based on our members' experiences responding to the Change Healthcare cyberattack, we urge CISA to consider ways to better clarify new reporting requirements and reduce burden on essential hospitals. We offer the following comments for the agency's consideration.

## 1. The criteria for "substantial cyber incident" should be clarified for efficient, accurate reporting.

The definition of "substantial cyber incident" in the proposed rule is vague and may result in reporting of cybersecurity incidents that are not relevant to CISA's intended purpose. The Proposed Rule at § 226.1 gives four criteria that may define a "substantial cyber incident;" however, the use of qualifiers in these criteria is inconsistent. The lack of definition for qualifiers such as "substantial" and "serious" makes it unclear whether reporting would be required for instances where a single account is comprised or there is minimal disruption to health care services.

Without a clear and precise definition, health care providers will be left to interpret what constitutes a "substantial cyber incident," which could lead to inconsistencies and potential underreporting or overreporting. This ambiguity also could create confusion and uncertainty, which would hinder hospitals' ability to effectively prioritize and respond to genuine cyber threats. Additionally, the lack of clarity might result in unnecessary administrative burdens, as hospitals may feel compelled to report minor incidents to avoid potential noncompliance.

**To ensure effective implementation and compliance, it is crucial for DHS and CISA to provide a clear, specific definition of "substantial cyber incident" that considers the unique operational context and resource constraints of essential hospitals, enabling them to focus on truly significant threats that affect patient care and safety.** We urge DHS and CISA to refine the criteria for what constitutes a "substantial cyber incident" to ensure clarity and efficient, accurate reporting that aligns with essential hospitals' unique operational context and resource constraints.

## 2. Essential hospitals should have more time and flexibility to implement CIRCIA reporting requirements because of their unique operational demands and resource constraints.

Essential hospitals require flexibility to prioritize patient care and immediate response to ongoing threats. Imposing strict 72-hour and 24-hour deadlines for reporting cyber incidents and ransom payments could divert critical resources away from patient care and essential medical services during a crisis. This is exacerbated by the limited cyber workforce in the health care sector. Furthermore, hospitals may need more time to thoroughly assess the scope and impact of a cyber incident, ensuring accurate and comprehensive reporting. **A more flexible timeline would allow hospitals to balance the urgent needs of patient care with the necessity of reporting, ultimately fostering a more effective and sustainable cybersecurity response**.

Additionally, the extensive initial reporting requirements contained in § 226.6 and § 226.8 might lead to rushed, incomplete, or inaccurate information, potentially hindering effective incident response and recovery efforts. **A more streamlined and phased reporting process would allow hospitals to prioritize immediate cybersecurity and patient care needs, followed by thorough and accurate incident documentation once the immediate crisis is managed.** This approach not only would support better incident management but also ensure the integrity and usefulness of the reported information. We urge DHS and CISA to recognize the limited information that may be available to health care providers at the current 72-hour deadline and adjust the reporting process to ensure accurate and complete reporting of information.

The proposed regulation from DHS and CISA also represents an unfunded mandate, placing additional financial strain on essential hospitals without providing the necessary funding to support compliance. This lack of financial support is particularly problematic given the current shortage of cybersecurity professionals, which leaves hospitals struggling to meet both operational and regulatory obligations.[2] While essential hospitals have made significant progress in improving their health care cybersecurity programs, challenges arise related to limited cybersecurity budgets, insufficient staffing, and poor retention of cybersecurity professionals. **Alleviating these burdens by providing technical assistance, in addition to a simple extended and phased reporting process, would allow essential hospitals to better allocate their limited resources, ensuring that critical incidents are effectively managed without compromising patient care or financial stability.**

*******

America's Essential Hospitals appreciates the opportunity to submit these comments. If you have questions, please contact Director of Policy Rob Nelb, MPH, at rnelb@essentialhospitals.orgrnelb@essentialhospitals.org or 202-585-0127.

Sincerely,

Bruce Siegel, MD, MPH
President and CEO

[2] *2023 HIMSS Healthcare Cybersecurity Survey*. Healthcare Information and Management Systems Society. https://www.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf. Accessed May 31, 2024.