November 10, 2022

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane
Washington, D.C.

RE: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 [Docket ID: CISA–2022–0010]

Dear Director Easterly:

The Confidentiality Coalition appreciates the opportunity to submit comments on the Cybersecurity and Infrastructure Security Agency's (CISA) Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022 published in the Federal Register on September 12, 2022 (RFI)[1].

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective health information privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

Cybersecurity incidents are a significant challenge for healthcare stakeholders. In 2021, over 45 million individuals were impacted by cyber attacks on healthcare entities, a record amount.[2] Of the 16 sectors categorized as "critical infrastructure," healthcare companies reported the greatest number of ransomware attacks in 2021.[3] These attacks are not only harmful to

[1] 87 Fed. Reg. 55833 (September 12, 2022).
[2] Heather Landi, *Healthcare data breaches hit all-time high in 2021, impacting 45M people*, Fierce Healthcare (February 1, 2022), https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people.
[3] *Internet Crime Report 2021*, Federal Bureau of Investigation Internet Crime Complaint Center (March 23, 2022), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

organizations in terms of financial cost[4] and the unauthorized release of sensitive information but can disrupt operations and put the health and safety of patients in jeopardy.

The Confidentiality Coalition thanks CISA for its work to improve cyber resilience by offering tools and logistical support to confront current and future threats to healthcare infrastructure. We recognize and support the need for the government to obtain more information about cybersecurity incidents to help prevent them, and encourage CISA to share as much information as possible with covered entities to assist them in responding to such incidents.

We recommend that CISA coordinate any reporting requirements with other federal agencies, such as the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC), in order to avoid duplicate incident reporting as much as possible. The healthcare industry must already comply with an extensive array of state and federal cyber, security and privacy data breach reporting requirements. Federal requirements, for example, include regulations implementing the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH Act), including reporting certain data breaches to the HHS Office for Civil Rights' (OCR) pursuant to the HIPAA Breach Notification Rule and to the FTC pursuant to the FTC Breach Notification Rule. These rules have been in place for several years and have been successful in ensuring that the government is apprised of all material data breaches in the health care industry. Consistent with the requirement in CIRCIA for CISA to not require reporting from a covered entity where that covered entity is required by law, regulation, or contract to report substantially similar information to another federal agency within a substantially similar timeframe, we ask that CISA consider the extent to which its reporting requirements may be harmonized with those of OCR and the FTC such that a given incident need only be reported to a single federal agency. In addition to federal requirements, currently 21 states have cybersecurity breach reporting laws and all states have data breach reporting laws. To the extent that CISA can leverage existing federal and state cyber incident and data breach reporting requirements for consistency and to reduce the burden on covered entities, we urge it to do so.

We also ask that CISA allow a delay in reporting under CIRCIA if a covered entity is working with law enforcement. HIPAA, for example, allows for a reporting delay if a law enforcement official indicates that a notification, notice, or posting required under HIPAA would impede a criminal investigation or result in harm to national security. Failing to allow a law enforcement delay for notification by law enforcement would result in a conflict with the reporting requirements under HIPAA and the FTC Breach Reporting Rule, and could undermine the efforts of law enforcement, HIPAA, and increase the risk of harm to the covered entity, the overall healthcare industry, impacted individuals, state and/or federal investigations, and national security.

[4] Heather Landi, *Average cost of healthcare data breach rises to $7.1M, according to IBM report*, Fierce Healthcare (July 29, 2020), https://www.fiercehealthcare.com/tech/average-cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report.

The Confidentiality Coalition looks forward to working with CISA on the implementation of the CIRCIA cyber incident reporting requirements and its other efforts to improve cybersecurity readiness. Included is a copy of the Confidentiality Coalition's principles on cyber incident reporting. Please contact me at tgrande@hlc.org or 202-449-3433 with any questions.

Sincerely,

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council