November 14, 2022

Submitted via the Federal rulemaking Portal: http://www.regulations.gov

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

RE: Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 [CISA2022-0010)

Dear Director Easterly:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) appreciate the opportunity to comment on the Cybersecurity and Infrastructure Security Agency (CISA) Request for Information (RFI)[1] to receive input from the public as CISA develops proposed regulations required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as published in the *Federal Register* on September 12, 2022 (Vol. 87, No. 175).

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders in hospitals, health systems and other healthcare settings across the country. Consisting of more than 2,900 members in 60 countries, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents nearly one thousand healthcare security leaders and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and the security of patient and provider data and devices connecting to their networks.

Key Recommendations and Takeaways

CHIME and AEHIS are pleased to provide input in response to this RFI, as CISA begins to develop and oversee implementation of regulations requiring covered entities to submit reports detailing covered cyber incidents and ransom payments. We believe the following areas are especially important for CISA to consider when creating the policies and provisions related to mandatory cybersecurity information sharing:

1. **Reducing Reporting Redundancy:** The granularity of data that must be reported must be balanced against what is already mandated under existing laws (e.g., the Health Insurance Portability and Accountability Act (HIPAA)), and any future federal reporting requirements.
2. **Balanced Reporting Requirements:** Data reporting requirements should be balanced and factor in the following considerations:
    a. Minimize data reporting to only what is absolutely necessary;

[1] 87 Fed. Reg. 55833 (September 12, 2022).

   b. "Covered entities" (as yet to be defined) in the healthcare critical infrastructure sector should only be required to report details after initial mitigation and response efforts;
   c. Reporting a cyber incident should be permitted to occur by both phone and electronic reporting – and the agency should set up a hotline to help facilitate reporting and questions related to compliance;
   d. Data reporting should be tailored to sector-specific needs;
   e. CISA should proactively work with partner federal agencies to define the "front door" for reporting purposes;
   f. There should be a bi-directional exchange of information and the data must be made freely available to the entire healthcare ecosystem;
   g. Federal agencies should collaborate and coordinate if an incident is reported outside of CISA, in order to avoid shifting/adding reporting burdens back to healthcare providers;
   h. Encouraging entities to report their data using as standard protocol should be encouraged but not mandated where infeasible;
   i. Data must be made freely available to the healthcare ecosystem; and
   j. CISA should partner with sector-specific ISACs to determine a plan by which the information will be distributed back to the sectors
3. **Smaller and Lesser-Resourced Providers:** Healthcare providers – particularly smaller and under-resourced providers – must not be penalized for reporting less granular data.
4. **Prioritizing Patient Safety:** Data reporting requirements during a catastrophic cybersecurity incident ("covered incident") should not be prioritized over patient safety.

The Current Healthcare Cyber Threat Landscape

Cyberattacks pose a persistent threat to patient safety and our national security. As one of our members stated in testimony to the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality and Security last year, "Cybersecurity incidents are not only a threat to national security, they are also a threat to patient safety, as attacks can cause denial of service, medical device corruption, and data manipulation that directly impacts clinical operations, patient care and public health. In addition, healthcare data and information remain lucrative targets for theft and exploitation, particularly through ransomware attacks and COVID themed social engineering by criminal groups and adversarial nation states."[1] The techniques used are the same ones that have been successfully used against large, publicly traded companies with far greater resources than most healthcare providers.

Between 2009 and 2021, 4,419 healthcare data breaches of 500 or more records have been reported to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR). Those breaches have resulted in the loss, theft, exposure, or impermissible disclosure of 314,063,186 healthcare records – equating to nearly 95 percent of the 2021 population of the United States. In 2021, an average of 1.95 healthcare data breaches of 500 or more records were reported each day, double the number of reported breaches only four years prior.[2] When hackers and/or bad actors gain access to patient records and information, they will have the ability to change and manipulate patient data – which could have disastrous consequences to each individual patient. Two out of three of respondents to CHIME and AEHIS's cybersecurity survey reported having had a security incident occur in the past 12 months.

[1] *The National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality and Security Hearing*. (July 21, 2021). National Committee on Vital and Health Statistics. Retrieved October 25, 2022, from https://ncvhs.hhs.gov/meetings/subcommittee-on-privacy-confidentiality-and-security-3/.*Testimony of Erik Decker*. Retrieved October 25, 2022, from https://chimecentral.org/wp-content/uploads/2021/07/1A-Decker-WrittenTestimony-only.pdf

[2] *Healthcare Data Breach Statistics - Latest Data for 2022*. (2022, August 26). HIPAA Journal. Retrieved October 25, 2022, from https://www.hipaajournal.com/healthcare-data-breach-statistics/

In order to better understand the current cybersecurity challenges facing healthcare providers we polled our membership in a survey[3] to better understand the threats our member organizations face, the resources they need and the education gaps that currently exist. The results continue to support what those who have been active in the cybersecurity landscape have known for years, healthcare is under constant threat, more resources are needed for healthcare providers and significant education gaps remain.

Detailed Recommendations

Definitions and Applicability

Pursuant to the CIRCIA law, "A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered **cyber incident** has occurred." Furthermore, "**A covered entity** that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made." CIRCIA furthermore says a "cyber incident" "has the meaning given the term 'incident' in section 2209; and ''(B) does not include an occurrence that imminently, but not actually, jeopardizes— ''(i) information on information systems; or ''(ii) information systems."[4]

The statute defines a significant cyber incident to be: "a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States." Finally, CIRCIA also establishes a definition for "substantial cyber incident" to mean, "a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States."

Healthcare providers are under constant attack and are fending off relentless cyberattacks on a daily basis. CHIME and AEHIS members believe it would overwhelm our sector, as well as CISA, if covered entities were required to report to CISA cyber incidents other than ones designated as "substantial." Therefore, we strongly recommend that CISA: 1) only require that "substantial" events be required to be reported; 2) events that are a direct threat to patient safety be required to be reported; 3) that healthcare providers have the authority to use their discretion to ascertain to their best ability whether a threat is indeed a "substantial cyber incident"; and 4) should healthcare providers determine after a review that exceeds 72 hours that a cyber incident is, indeed, "substantial" – that reporting it after this timeframe is permitted, and should not result in any penalization (e.g., subpoenas and/or being reported to the U.S. Department of Justice (DOJ) for enforcement.)

Additionally, our members seek clarification from CISA on whether not-for-profit (NFP) entities will be subject to mandatory cyber reporting requirements. CIRCIA defines a "covered entity" to be, "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 2242(b)." According to Presidential Policy Directive 21[6], this includes public and private entities. Given that most hospitals and healthcare delivery organizations (HDOs) are not-for-profit entities, we would appreciate clarification from CISA on whether they consider them to be private entities, and thus subject to the mandatory cyber reporting requirements.

[3] *Survey of Members*. The College of Healthcare Information Management Executives (CHIME) and The Association for Executives in Healthcare Information Security **(**AEHIS). August 2021. https://chimecentral.org/wpcontent/uploads/2021/08/PP_infographic-v5_Handout.pdf

[4] Section 2209 of the Homeland Security Act of 2002 defines a cyber an incident to be "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system." [6] *Presidential Policy Directive -- Critical Infrastructure Security and Resiliance*. (2013, May 23). whitehouse.gov. Retrieved October 31, 2022, from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidentialpolicy-directive-critical-infrastructure-security-and-resil

Data Reporting

In considering what data elements and information must be reported to CISA, our members recommend that the agency take into account several factors:

1. Data reporting requirements should be limited to include only what information is necessary to facilitate the spirit of the law which is sharing threat information to help avert other attacks.
2. We urge CISA to recognize that a healthcare provider may be unaware of whether a cyber incident is a "state-sponsored attack" until a more thorough review of the incident is completed. "Covered entities" (as yet to be defined) in the healthcare critical infrastructure sector should only be required to report details after the initial mitigation and response efforts. It is also important to note that an entity may not know all vulnerabilities that were exploited in an attack at the time of the incident. Sufficient forensic investigation is required to establish a full root cause analysis and/or kill chain of the attack. Initial forensic efforts are targeted at containment planning and validation to allow for recovery to begin. CISA should consider allowing for an initial reporting with the ability to update the report overtime as more forensic evidence and analysis becomes available.
3. CISA should permit both phone and electronic reporting, and the agency should set up a hotline to help facilitate reporting and questions related to compliance.
4. Data reporting should be tailored – when necessary – to sector-specific needs. For example, understanding whether the vulnerability involved a medical device, and if so, which one(s). It should also detail vulnerabilities located elsewhere in a networked environment such as heating, ventilation and air conditioning (HVAC) systems. To be clear, though, requiring reporting of information beyond what is needed to help facilitate information sharing to avert other possible related cyberattacks should be avoided.
5. CISA should proactively work with partner federal agencies to define the "front door." If CISA expects reporting within 72 hours, we believe it should also be CISA's responsibility to notify other federal authorities like the Federal Bureau of Investigations (FBI).
6. If reporting is made to a federal agency other than CISA (e.g., the FBI), then it should be incumbent on that agency to share the threats with CISA without shifting the burden back to the health care provider and penalizing healthcare providers in these situations should be avoided.
7. There should be a bi-directional exchange of information and the data must be made freely available to the entire healthcare ecosystem – which includes all sizes of healthcare providers, payers, pharmaceutical/life sciences organizations, medical device manufacturers and other third-party vendors and suppliers.
8. Encouraging entities to report their data using a standard protocol (i.e., standards developed in an effort to improve the prevention and mitigation of a cyber incident). This will enable automated tools to process the data in a manner that provides operational efficiencies and effectiveness. A standard protocol should only be encouraged where feasible; it is essential that CISA take into consideration that smaller and lesser-resourced entities may not have these capabilities.
9. CISA should partner with sector-specific Information Sharing and Analysis Centers (ISACs) to determine a plan by which the information will be distributed back to the sectors. Sectors should have access to information sharing sourced from sector, and from other sectors which may have cross sector impact. CISA should have responsibility to work with ISACs to reduce burden of duplication of information sharing mediums and data should be made available in industry standard threat intelligence sharing formats (e.g., Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXXI)).
10. CISA should define and provide information, services and/or support that may be made available from the agency to the covered entity in response to the incident report.

Avoid Duplicative Reporting

CHIME and AEHIS have long supported the need for stronger information sharing practices. While the Cybersecurity Information Sharing Act of 2015[5] took a big step in this direction by authorizing healthcare information sharing in certain situations. However, healthcare entities are often apprehensive to do so

[5] Pub. L. No. 114-113

because they worry about running afoul of HIPAA rules or suffering significant reputational harm. While suffering a cyber incident resulting in a HIPAA breach can create harm to reputation, we also believe it is

imperative that providers be able to share threats in order to assist in averting potentially catastrophic patient safety incidents. **Nonetheless, CHIME and AEHIS believe that to the degree possible, any duplicative reporting that is currently required under other federal policies (described in more detail below) should be avoided.**

Under Section 2242(5)(B) of CIRCIA[6], pertaining to "Required Reporting of Certain Cyber Incidents", there is an "Exceptions" provision for "Substantially Similar Reported Information." It states: "(i) IN GENERAL.—Subject to the limitation described in clause (ii), where the Agency has an agreement in place that satisfies the requirements of section 104(a) of the Cyber Incident Reporting for Critical Infrastructure Act of 2022, the requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe. **Therefore, consistent with this 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 the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) such that a given incident need only be reported to a single federal agency.**

The healthcare industry is already required to comply with a myriad of both state and federal cyber, security, and privacy data breach reporting requirements. These include federal authorities and requirements under HIPAA regulations and the Health Information Technology for Economic and Clinical Health (HITECH Act) regulations. Specifically, the HIPAA Breach Notification Rule[7], as well as the HITECH Act's additional data breach reporting requirements to the HHS' OCR[8], and the FTC's Health Breach Notification Rule.[9] At the state-level, in 2021, at least 45 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity; and at least thirtysix states enacted bills in the same year.[10] In 2022, at least 40 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity; and twenty-four states enacted at least 41 bills in 2022 so far.[11]

CHIME and AEHIS would also appreciate significant consideration and clarification in the proposed rulemaking regarding the intersection of the potential future proposed rule regarding "Mandatory Cyber Incident Reporting" and existing federal and state laws, regulations and oversight. We strongly recommend that DHS and CISA coordinate with other federal agencies with existing jurisdiction – including HHS, HHS' OCR, and the FTC – to ensure that duplicative cyber incident reporting requirements are avoided to the greatest extent possible. **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 strongly urge it to do so.**

CISA states that they are "particularly interested in input on definitions for and interpretations of the terminology to be used in the proposed regulations; the form, manner, content, and procedures for submission of reports required under CIRCIA; information regarding other incident reporting requirements

[6] Consolidated Appropriations Act, 2022. Pub. L. No. 117-103, § 2242(5)(B). https://www.congress.gov/bill/117thcongress/house-bill/2471

[7] *Breach Notification Rule*. (2021, June 28). HHS.gov. Retrieved October 31, 2022, from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

[8] Breach Notification for Unsecured Protected Health Information. 74 FR 42739 and 74 FR 42767, Aug. 24, 2009, Retrieved October 31, 2022 from https://www.federalregister.gov/documents/2009/08/24/E9-20169/breachnotification-for-unsecured-protected-health-information

[9] Federal Trade Commission's Health Breach Notification Rule, 16 C.F.R. Part 318

[10] *Cybersecurity Legislation 2021*. (n.d.). Retrieved October 31, 2022, from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation2021.aspx

[11] *Cybersecurity Legislation 2022*. (n.d.). Retrieved October 31, 2022, from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2022637922035.aspx

including the requirement to report a description of the vulnerabilities exploited; and other policies and procedures, such as enforcement procedures and information protection policies, that will be required for implementation of the regulations." **Therefore, we strongly urge CISA to host a series of stakeholder meetings to garner feedback from the healthcare industry, specifically, before promulgating a proposed rule. It is critical that the proposed regulations do not inadvertently create overly duplicative requirements, penalize healthcare providers unfairly, and add burden to an already highly regulated sector of our critical infrastructure. CHIME and AEHIS members are executives and senior healthcare IT leaders – and we are offering to serve as a resource to CISA throughout this process. Our members are extremely knowledgeable and have decades of experience executing cybersecurity best practices, as well as real-world experience dealing with the ramifications of cyberattacks.**

CHIME and AEHIS respectfully request that CISA allow a delay in reporting under CIRCIA in instances where "covered entities" in the healthcare critical infrastructure sector are already working with law enforcement. For example, HIPAA[14] 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. Covered entities (as defined under HIPAA) may disclose protected health information (PHI), without the individual's authorization, to a public health authority acting as authorized by law in response to a bioterrorism threat or public health emergency.[15]

The Privacy Rule also permits a covered entity to disclose protected health information to public officials who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism[16] in order to avert a serious threat to health or safety. In addition, disclosure of PHI, without the individual's authorization, is permitted where the circumstances of the emergency implicates law enforcement activities.[17] **If CISA promulgates rulemaking which fails to allow a law enforcement delay for notification by law enforcement, it would result in a direct conflict with the reporting requirements under HIPAA and the FTC Breach Reporting Rule. Furthermore, it 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.**

Prioritize Patient Safety

Patient safety in the healthcare sector means not just ensuring access to care, but ensuring that patient safety is not jeopardized. Adding an additional requirement to provide detailed reporting of all the vulnerabilities exploited during a catastrophic incident should not be prioritized over patient safety. Therefore, considerations should be given to the three-day reporting mandate and what precisely is required during this time period – when a provider is appropriately prioritizing and triaging patients during the impacted window.

A recent study found that about half (45 percent) of cyberattacks resulted in adverse impact on patients. About half (53 percent) of those with adverse impacts on patient care report increased mortality rates after a cyberattack (24 percent overall). About half (56 percent) have experienced one or more cyberattacks in the last 24 months. Almost half (43 percent) have experienced at least one ransomware attack in the last 24 months. When cyberattacks result in adverse patient care, patients face risks including high rates of impacted service (54 percent) and inappropriate therapy or treatment deliveries (26 percent). Furthermore, "for every reported set of vulnerabilities related to hospital robots or infusion pumps, there are likely thousands more that are unknown and far more dangerous."[6]

[14] *397-Does HIPAA permit covered entities to disclose information to public officials responding to a public health emergency*. (2021, June 28). HHS.gov. Retrieved October 31, 2022, from https://www.hhs.gov/hipaa/forprofessionals/faq/397/does-hipaa-permit-covered-entities-to-disclose-information-to-officials-responding-to-publichealth-emergencies/index.html

[15] 45 CFR 164.512(b))

[16] 45 CFR 164.512(j))

[17] 45 CFR 164.512(f)); national security and intelligence activities. 45 CFR 164.512(k)(2)); or judicial and administrative proceedings.45 CFR 164.512(e)).

Small and Lesser-Resourced Providers

Many hospitals are under-resourced, and some do not even have a single, full-time employee devoted to the oversight of cybersecurity even as threats have escalated year after year. **With the health sector only as strong as its weakest link, it is imperative that CISA prioritize assisting smaller and lesser resourced providers in fending off growing and sophisticated attacks aimed at stealing intellectual property, extorting ransoms, threatening patients by targeting medical devices and hindering their ability to deliver care overall.**

Prioritize Education

CHIME is strongly supportive of and grateful that CISA offers a range of resources – including cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework. These professional, no-cost assessments are provided upon request on a voluntary basis and can help any organization with managing risk and strengthening the cybersecurity of our Nation's critical infrastructure.[12] The ability to rapidly respond to cybersecurity incidents – and when possible, preventing them – while sharing information with our federal partners is essential to protect hospitals and healthcare delivery organizations (HDOs).

Conclusion

In closing, CHIME would like to thank you for providing the opportunity to comment on this CISA RFI. As CISA continues to garner input from the public in developing proposed regulations required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), CHIME and our members would appreciate continued opportunities to help inform the important work being done by CISA. We look forward to continuing to be a trusted stakeholder and resource to you and continuing to deepen the longstanding relationship we have shared. Working together through the rulemaking process, such as with the RFI, is just one way we can accomplish our shared goals and make meaningful changes in healthcare.

Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Director, Federal Affairs at carnone@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME

[12] *Cyber Resource Hub | CISA*. (n.d.). Retrieved October 31, 2022, from https://www.cisa.gov/cyber-resource-hub