July 3, 2024

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: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements [CISA-2022-0010]

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's (CISA) proposed rule required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as published in the *Federal Register* on April 4, 2024 (Vol. 89, No. 66, 89 FR 23644).

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

CIRCIA, as amended, requires CISA to promulgate regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities. CISA is seeking comment on the proposed rule to implement CIRCIA's requirements and on several practical and policy issues related to the implementation of these new reporting requirements. CHIME and AEHIS are pleased to provide input in response to this proposed rule. Additionally, you can find CHIME and AEHIS's response to CISA's 2022 Request for Information (RFI) on the proposed rulemaking here.

CISA is proposing to include in the description of covered entity multiple sector-based criteria related to the Healthcare and Public Health (HPH) Sector. CISA is also proposing requiring

reporting from larger hospitals (i.e., those with more than 100 beds) and critical access hospitals (CAHs). Throughout our comment letter, we use the terms *HPH Sector*, *hospitals and healthcare systems*, *healthcare delivery organizations (HDOs)*, and *providers* interchangeably on behalf of our members. As noted, CHIME and AEHIS represent executive and senior healthcare IT leaders within the HPH Sector – specifically in hospitals, health systems and other healthcare settings.

We believe the following areas are especially important for CISA to consider when finalizing this proposed rule:

- CHIME and AEHIS members believe strongly that cybersecurity is patient safety, and regulatory requirements should not jeopardize their core mission of care.
- We must continue to move away from a mentality that punishes those that have been victimized by malicious actors and criminals.
- Our members strongly recommended that DHS and CISA coordinate with other federal agencies with existing jurisdiction – including the U.S. Department of Health & Human Services (HHS), HHS' Office for Civil Rights (OCR), and the Federal Trade Commission (FTC) – to minimize duplicative cyber incident reporting requirements to the greatest extent possible.
    - CISA's proposed inclusion of "substantial loss of confidentiality" in the definition of a "substantial cyber incident" could add burden on hospitals and healthcare systems by creating duplicative requirements in an existing complicated regulatory framework.
- As proposed, hospitals and healthcare systems are concerned that OCR may treat a CIRCIA Report as acknowledgment of a data breach – regardless of its actual reportability under the Health Insurance Portability and Accountability Act (HIPAA). Thus, the HIPAA reporting timelines could be triggered upon the submission of a CIRCIA Report, creating potential compliance challenges and additional burdens for our members.
- Cybersecurity is a shared responsibility, therefore, CISA should clarify that when a substantial cyber incident occurs at the level of a managed service provider or other third-party service provider, if that organization serves, contracts with, or is otherwise legally engaged with any entities in a critical infrastructure sector, that the third-party service provider must be the covered entity to fulfill any and all CIRCIA reporting obligations.
    - This proposal places the onerous solely on our members as covered entities, rather than third-parties – who may or may not be covered entities.
- Data reporting requirements should be limited to include only what information is minimally necessary, a cybersecurity best practice. This will also facilitate the spirit of CIRCIA – which is sharing threat information to help avert other cyberattacks.
- As proposed, hospitals and healthcare systems are required to provide detailed and numerous reports during, throughout, and after a substantial cyber incident. Our members believe strongly that the supplemental reporting and timing of "without delay or as soon as possible" will mean that ensuring compliance with these reporting requirements could be prioritized over patient safety.
    - While CHIME and AEHIS appreciate that CISA is proposing to allow for supplemental reporting after a substantial cyber incident – which we supported in our response to the RFI – we have significant concerns.
    - We are recommending that hospitals and healthcare systems must be permitted to submit supplemental reports every 72 hours at minimum, or every five business days. This reporting cadence would be required only when and if substantial new or different information becomes available.

- CISA is proposing size-based criteria; our members believe that rather than allowing certain entities to "self-assess" if they meet this criteria, CISA must include health insurance companies, third-party administrators (TPAs) of health plans, and healthcare clearinghouses in the HPH Sector-based criteria. We are extremely concerned that if these third-parties are not explicitly "carved-into" the HPH Sector-based criteria, that they may simply self-assess that they do not meet the proposed size-based criteria, and are not subject to CIRCIA.
    - CHIME and AEHIS members have been victims due to cyberattacks on third-party services or breaches affecting their vendors and contractors. There is no greater example of the devastating impact this can have on healthcare than the unprecedented cyberattack on Change Healthcare this year – which is a clearinghouse and unit of a health insurance company – UnitedHealth Group (UHG).
    - These third-parties hold vast quantities of patient data and are integral partners in the healthcare ecosystem. If CISA is to achieve the purpose of CIRCIA, and truly enhance the security and resiliency of the nation's critical infrastructure, CHIME and AEHIS believe that the final rule must include the above listed third-parties, at minimum.
- CISA is proposing, under the HPH Sector-based criteria, to include requiring reporting from larger hospitals (i.e., those with more than 100 beds) and CAHs. Certain factors and complexities – as outlined in our comments below – underscore the inadequacy of using a single criterion such as "hospitals with 100 beds or more" to determine hospital size capacity. Rather, we suggest that a more nuanced approach, considering multiple criteria beyond just bed count, to accurately characterize hospital size and capacity.
    - Further, CHIME and AEHIS believe that CISA's proposed scope to include CAHs is not appropriate at this time. Imposing additional regulatory burdens on rural hospitals could inadvertently increase their financial and operational strain, leading to more closures and reduced access to healthcare – and crucially – could divert resources away from patient care.
- CISA is proposing to offer a web-based form as the manner of submission of CIRCIA Reports, and our members broadly agree with this approach. However – we strongly believe that covered entities should be able to test the proposed web-based forms before the issuance of the final rule, for all four of the proposed CIRCIA Reports.
    - Our members strongly recommend that CISA implement a sandbox environment version of the web-based forms for each of the Reports well in advance of deploying them for reporting purposes. Initially isolating the forms in a controlled environment so that they can be executed and tested safely without risking any of the overall systems and networks is essential.
    - As our members are executives and senior healthcare IT leaders – we are offering to serve as a resource to CISA throughout this process. They are extremely knowledgeable and have decades of experience executing cybersecurity best practices, as well as real-world experience dealing with the ramifications of cyberattacks. Our members are able and willing to provide input on the forms, and are offering to serve as "beta-testers."
- CHIME and AEHIS members are extremely concerned about the proposed § 226.8(d), which would require "a description of the covered entity's security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the incident." If CISA requires hospitals and healthcare systems to define their entire security architecture, that is a tremendous amount of information to include in a report. Our members do not believe that CISA needs to know an entire description of an

organization's security program – as it is not helpful to fulfill the purpose of CIRCIA, is potentially considered intellectual property (IP), and/or sensitive for the organization.
    - Further, if the entire security architecture of a hospital or healthcare system is sent to CISA, it is the most target rich information for bad actors. Our members believe that the other proposed reporting requirements would be more than sufficient for CISA to share necessary threat information.
    - The proposed language "including but not limited to" should be stricken from the final rule and changed to "only including" – so that § 226.8(d) reads "A description of the covered entity's security defenses in place, only including any controls or measures that resulted in the detection or mitigation of the incident."
- This proposal's lack of details on how, specifically, CISA plans to fulfill fundamental obligations required by CIRCIA, is disappointing, and does not allow for CHIME and AEHIS members to offer meaningful feedback or input. In the proposal, CISA asserts that the information reported to them "will enable CISA to carry out its core statutory responsibilities related to identifying and sharing information on cyber incident trends, TTPs, vulnerability exploitations, campaigns, and countermeasures that may be useful in preventing others from falling victim to similar incidents and preventing similar vulnerability classes in the future."
    - All of the outcomes and benefits that CISA describes rely on timely, adequate, and bi-directional information distribution. CISA should have provided details in this proposal, specifically regarding how they plan to partner with SRMAs and sector-specific ISACs to determine a plan by which the information will be distributed back to the sectors.
    - 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 HDOs.

Overview: The Cybersecurity Landscape in the Healthcare & Public Health (HPH) Sector

Hostile nation states have grown increasingly aggressive with their tactics, attacking hospitals and other healthcare stakeholders daily. This poses an imminent risk to our national defense. Bringing down a hospital or multiple HDOs at once is a risk for the nation and it shakes the confidence and trust of everyday Americans which is precisely what hostile nation states intend. They are looking to exact physical, financial, and psychological harm.

According to a recent Fact Sheet from the White House: "Recent cyberattacks targeting the nation's healthcare system have demonstrated the vulnerability of our hospitals and payment systems. Providers across the health system had to scramble for funding after one attack on a key payment system. And some hospitals had to redirect care after another. These disruptions can take too long to resolve before full access to needed health care services or payment systems is restored. Cyberattacks against the American healthcare system rose 128% from 2022 to 2023."[1]

Healthcare data and patient information remain lucrative targets for theft and exploitation, particularly through ransomware attacks. Criminal groups and adversarial nation states utilize tactics, techniques and procedures (TTPs) across our Sector – including large, publicly traded

[1] *FACT SHEET: Biden-Harris administration bolsters protections for Americans' access to healthcare through strengthening cybersecurity*. The White House (11 June 2024). https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/10/fact-sheet-biden-harris-administration-bolsters-protections-for-americans-access-to-healthcare-through-strengthening-cybersecurity/

companies with far greater resources than most U.S. hospitals and health systems. Healthcare continues to experience the highest data breach costs of all industries, increasing from $10.10 million in 2022 to $10.93 million in 2023 – an increase of 8.2 percent. Over the past three years, the average cost of a data breach in healthcare has grown 53.3 percent, increasing more than $3 million compared to the average cost of $7.13 million in 2020. As a comparison, the costs for a financial entity to recover from a breach are estimated to be $5.90 million.[2]

Our members are committed to adopting cybersecurity best practices and take their responsibility to protect not only the privacy and security of patient data and devices networked to their system – but critically – their patient's overall safety and well-being very seriously. Cyber safety is patient safety. Currently, hospitals are forced to balance the challenges of the high cost of cyber insurance, near-constant cyberattack attempts, the inherent risks to their patients, the weaponization of artificial intelligence (AI), and the current workforce shortage needed to mitigate all of these risks.

They are doing their best to navigate an ever increasingly complex cybersecurity landscape, a job that has become infinitely more complicated with managing third-party risk. Hospitals and healthcare systems must offer a wide range of services that require specialized skills and equipment, operate efficiently, and provide high-quality patient care. Thus, they must contract with third-parties – including medical device manufacturers, information and information technology (IT) companies, data storage companies, and others – which inherently introduce risk into their ecosystem. Our members often encounter third-parties that are unwilling to sign HIPAA business associate agreements (BAAs), and/or resist acceptance of appropriate levels of liability that recognize the great amounts of protected health information (PHI) they process and maintain.

While healthcare providers exercise due diligence processes when selecting third-party solutions or offerings, as well as ensure that sufficient administrative safeguards are in place, they are forced to deal with an overall lack of third-party willingness to offer indemnification clauses (i.e., "hold harmless") or limitations of liability in case of data breaches. If any limitation of liability is included, it is woefully inadequate. Thus, a disproportionate amount of risk is shouldered by providers.

According to HHS' OCR, "Ransomware and hacking are the primary cyber-threats in health care. Over the past five years, there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware. In 2023, hacking accounted for 79% of the large breaches reported to OCR. The large breaches reported in 2023 affected over 134 million individuals, a 141% increase from 2022."[3] In 2022, there were 707 data breaches, more than half of which occurred against third party service providers that handle PHI.[4]

Additionally, the costs of delivering care continue to increase at an unsustainable rate. While all subsectors in healthcare are feeling cost pressures, HDOs are facing:

- Increasing operating costs such as inflation and labor shortages;
- Impact of cybersecurity events such as ransomware and data breaches;

---

[2] *Cost of a data breach 2023 | IBM*. (n.d.-b). https://www.ibm.com/reports/data-breach

[3] HHS OCR (2024, February 21). HHS' Office for Civil Rights Settles Second Ever Ransomware Cyber-Attack. *HHS.gov*. https://www.hhs.gov/about/news/2024/02/21/hhs-office-civil-rights-settles-second-ever-ransomware-cyber-attack.html

[4] Garcia, G. & Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group. (2023). *In need of a checkup: Examining the cybersecurity risks to the healthcare sector* (By United States Senate Committee on Homeland Security and Government Affairs). https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Garcia-2023-03-16.pdf

- Continued downward pressure on hospital, physician practice, and smaller HDO reimbursements; and the
- Push from “Fee for Service” to “Value-Based” contracts.[5]

These factors in turn drive increased mergers, acquisitions, & divestitures (MA&D) and consolidation activities; focus on cost reduction; closures / reduced options for health services, especially in rural areas; and an increase in out-of-data / out-of-support vulnerable technologies. Nevertheless, CHIME and AEHIS members undertake and devote significant resources to securing their networks and systems because they are truly committed to the health, well-being, and safety of patients in the communities they serve.

Like nearly all organizations in the United States, hospitals and HDOs must care – to some degree – about their ability to generate positive net revenue in order to keep their doors open. However, they are unlike other organizations in that their first and most important mission is to care for their patients. Hospitals and healthcare systems are not only critical to the communities in which they serve, they are also often the largest employers.

We must continue to move away from a mentality that punishes those that have been victimized by malicious actors and criminals. Cybersecurity is a shared responsibility; however, without additional assistance, many of our members are limited in what they can do.

Cyber Incident, Covered Cyber Incident, and Substantial Cyber Incident – Definitions

CISA is proposing to include in the regulation a definition of the term cyber incident. The definition of cyber incident is important as it will help bound the types of incidents that trigger reporting requirements for covered entities under the proposed regulation. CISA is proposing to define cyber incident to mean an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually jeopardizes, without lawful authority, an information system. **CHIME and AEHIS broadly agree with this definition.**

CIRCIA requires CISA to include within the proposed rule a definition for the term **covered cyber incident**.[6] Because CIRCIA requires covered entities to report only those cyber incidents that qualify as covered cyber incidents to CISA, this definition is essential for triggering the reporting requirement. **CISA is proposing to define the term covered cyber incident to mean a substantial cyber incident experienced by a covered entity. CHIME and AEHIS broadly agree with this proposed approach.**

Within CIRCIA, Congress defined a covered cyber incident as “a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 681b(b) of this title.”[1] CISA believes that defining a covered cyber incident to include all substantial cyber incidents experienced by a covered entity rather than some subset thereof is both consistent with the statutory definition of covered cyber incident and is the least complicated approach to defining covered cyber incidents.

[5] Health Sector Coordinating Council. (2024). Health Industry Cybersecurity – Strategic Plan (2024–2029). https://healthsectorcouncil.org/wp-content/uploads/2024/02/Health-Industry-Cybersecurity-Strategic-Plan-2024-2029.pdf

[6] 6 U.S.C. 681(3)

Under this approach, a covered entity simply needs to determine if a cyber incident is a substantial cyber incident for it to be reported, rather than having to perform an additional analysis to determine if a substantial cyber incident meets some narrower criteria for a covered cyber incident. As the term substantial cyber incident is not used in CIRCIA other than to help define a covered cyber incident, CISA does not see any benefit to having one set of requirements for what constitutes a substantial cyber incident and a separate set of requirements for which substantial cyber incidents experienced by a covered entity qualify as covered cyber incidents. **CHIME and AEHIS broadly agree with this approach.**

CISA is proposing to include within the rule a definition for the term substantial cyber incident. Given CISA's proposal to define a covered cyber incident as a substantial cyber incident experienced by a covered entity, CISA notes that the term substantial cyber incident is "essential to the CIRCIA regulation as it identifies the types of incidents that, when experienced by a covered entity, must be reported to CISA."

While CIRCIA does not define the term substantial cyber incident, it provides minimum requirements for the types of substantial cyber incidents that qualify as covered cyber incidents.[7] Consistent with these minimum requirements, CISA proposes the term substantial cyber incident to mean:

> *a cyber incident that leads to 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 is further proposing that a substantial cyber incident resulting in one of the listed impacts include any cyber incident regardless of cause, including, but not limited to, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; a supply chain compromise; a denial-of-service attack; a ransomware attack; or exploitation of a zero-day vulnerability.

CHIME and AEHIS members would be remiss if we did not point out that, as proposed, the definition of a "substantial cyber incident" seems to exclude the largest cyberattack on the healthcare sector to date. This is for several reasons; it is unclear if the unprecedented cyberattack on UHG/Change Healthcare would have been required to be reported under CIRCIA, if the final rule was in effect at the time. We are unable to ascertain that Change Healthcare would have fallen under or met the size-based criteria, and they are not specifically included in the sector-based criteria for the HPH Sector. Our members outline these concerns in further detail below.

As CISA notes, "confidentiality" refers to "***preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information*** [emphasis added]." CHIME and AEHIS members have concerns about the use of the term "confidentiality" as it is proposed to be included in the definition of "substantial cyber incident", as well as in the first of the four impact prongs (Substantial Loss of Confidentiality,

[7] 6 U.S.C. 681b(c)(2)(A)

Integrity, or Availability). "***Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes*** [emphasis added]."[8]

Further, the 405(d) Program, as mandated by Congress in the Cybersecurity Act of 2015[9], has already established a minimum set of voluntary cyber hygiene practices. Additionally, in P.L. 116-321 Congress defined "recognized security practices" to be:

> *the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title).*

As identified in the statute's definition, there are several standards, best practices and procedures currently in place and currently relied on by healthcare providers to implement enterprise risk management best practices. We strongly supported and endorsed this law as it incentivizes the adoption of cybersecurity practices by acknowledging that providers who have been acting in good faith should not be penalized by OCR.

As CISA notes in the proposed rule, "the concepts of confidentiality, integrity, and availability (CIA), often referred to as the "CIA triad," represent the three pillars of information security." The proposal cites definitions from a National Institute of Standards and Technology (NIST) publication,[10] noting that "confidentiality" refers to "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." "Integrity" refers to "guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity," and "availability" refers to "ensuring timely and reliable access to and use of information." **However, from the perspective of our members, these principles often overlap and sometimes conflict, requiring thoughtful implementation of any new cybersecurity policies.**

Furthermore, as noted in the NIST Cybersecurity Framework (CSF) 2.0 – cybersecurity and privacy are independent disciplines, although their objectives can overlap in certain circumstances.[11] As the NIST Privacy Framework[12] states: "Having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks."

Hospitals and healthcare systems are already subject to multiple overlapping reporting requirements for cyber incidents resulting in "a substantial loss of confidentiality." These requirements come in the form of state data privacy laws and the reporting requirements under HIPAA – discussed further below. The inclusion of confidentiality incidents within the definition of

[8] 45 CFR 164.304 "Confidentiality"
[9] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[10] NIST. *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, Special Publication 1800-25 Vol. A at 1 (Dec. 2020), https://csrc.nist.gov/pubs/sp/1800/25/final
[11] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. In *NIST CSWP 29* [Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[12] NIST. (2020). *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

a “substantial cyber incident” creates an additional duplicative reporting requirement for this class of incidents. These existing reporting requirements have unique timelines attached to different trigger points, and hospitals and healthcare systems will need to evaluate if a CIRCIA Report triggers reporting requirement timelines under HIPAA prematurely.

Further, substantial confidentiality incidents may derive from insubstantial cyber events. Many records might be exposed from the compromise of an email account, a misdirection of records, or a configuration error. These types of incidents represent substantial data confidentiality breaches, but there is not valuable intelligence on threat actor TTPs. Therefore, the inclusion of confidentiality in the definition of “substantial cyber incident” may result in a volume of low value reports that increase burden on hospitals and healthcare systems, as well as CISA staff without meeting the intent or deriving the value intended from CIRCIA. The primary purpose of CIRCIA is to help preserve national security, economic security, and public health and safety – as well as to assist the Federal government in understanding the cyber threat landscape and enabling the timely sharing of information to enhance cyber resilience.

Thus, as CISA is proposing to include in the definition of “substantial cyber incident” a cyber incident that leads to “a substantial loss of confidentiality,” we respectfully request that CISA recognize that this could inadvertently implement an additional set of burdensome practices for hospitals and healthcare systems – adding to the fragmented, complex regulatory frameworks that our members already must comply with. CHIME and AEHIS strongly believe that CISA should not adopt policies that inadvertently create overly duplicative requirements, penalize healthcare providers unfairly, and add burden to an already highly regulated industry.

Minimum Requirements for a Cyber Incident to be a Substantial Cyber Incident

The proposed definition contains the following elements: (1) a set of four threshold impacts which, if one or more occur as the result of a cyber incident, would qualify that cyber incident as a substantial cyber incident; (2) an explicit acknowledgment that substantial cyber incidents can be caused through compromises of third-party service providers or supply chains, as well as various techniques and methods; and (3) three separate types of incidents that, even if they were to meet the other criteria contained within the substantial cyber incident definition, would be excluded from treatment as a substantial cyber incident. Ultimately, CISA is proposing four types of impacts that, if experienced by a covered entity as a result of a cyber incident, would result in the incident being classified as a substantial cyber incident and therefore reportable under the CIRCIA regulation. Each of these impact types is described in its own prong of the substantial cyber incident definition.

CHIME and AEHIS believe that CISA should clarify that when a substantial cyber incident occurs at the level of a managed service provider or other third-party service provider, if that organization serves, contracts with, or is otherwise legally engaged with any entities in a critical infrastructure sector, that the third-party service provider must be the covered entity to fulfill any and all CIRCIA reporting obligations. From an operational viewpoint, the covered entity that experiences the substantial cyber incident would be the organization that would have the necessary information to complete any of the CIRCIA Reports, as proposed. Additionally, the third-party service provider would likely – or be expected to be aware of – the incident before its customers or other contracted organizations.

Guidance for Assessing Whether an Impact Threshold is Met

When evaluating whether a cyber incident meets one of the four proposed impact thresholds that would qualify it as a substantial cyber incident, CISA notes that a covered entity should keep in mind several principles. First, an incident needs to meet only one of the four prongs, not all four of the prongs, for it to be a substantial cyber incident. **While not ideal, it is fairly straightforward proposal, and thus, we agree with this approach.**

For an incident to qualify as a substantial cyber incident, CISA interprets CIRCIA to require the incident to "actually result" in one or more of the impacts described. **CHIME and AEHIS broadly agree with this approach.**

Additionally, CISA is proposing that the type of TTP used by an adversary to perpetrate the cyber incident and cause the requisite level of impact is typically irrelevant to the determination of whether an incident is a substantial cyber incident. **CHIME and AEHIS broadly agree with this approach.**

CISA has elected not to limit the definition of substantial cyber incident to impacts to specific types of systems, networks, or technologies. **CHIME and AEHIS broadly agree with this approach.**

CISA is aware that in some cases, a covered entity will not know for certain the cause of the incident within the first few days following the occurrence of the incident. CISA is proposing that a covered entity does not need to know the cause of the incident with certainty for it to be a reportable substantial cyber incident. **CHIME and AEHIS broadly agree with this approach.**

CISA states that: "For incidents where the covered entity has not yet been able to confirm the cause of the incident, the covered entity must report the incident if it has a "reasonable belief" that a covered cyber incident occurred. If an incident meets any of the impact-based criteria, it would be reportable if the covered entity has a "reasonable belief" that the threshold impacts occurred as a result of activity without lawful authority, even if the specific cause is not confirmed." **CHIME and AEHIS members have concerns regarding this proposal and the fourth prong, as outlined below.**

As proposed, we reiterate our concerns regarding the reporting timelines for a "confidentiality" breach, and the conflicting timelines for reporting under CIRCIA and HIPAA[16, 17, 18]. Data breach reporting under HIPAA is based on the confirmation of a data breach: "A covered entity must notify the Secretary if it discovers a breach of unsecured protected health information."[13] As proposed, CIRCIA reporting is based on "reasonable belief." The very real risk and burden to hospitals and healthcare systems is that OCR may treat a CIRCIA Report as acknowledgment of a data breach – regardless of its actual reportability under HIPAA. Consequently, the HIPAA reporting timelines could be triggered upon the submission of a CIRCIA Report, creating potential compliance challenges and additional burdens for our members. **In essence, the CIRCIA Report could prematurely initiate the HIPAA reporting obligations timeline, leading to confusion and undue administrative strain.**

Furthermore, under HIPAA, a covered entity's breach notification obligations differ based on whether the breach affects 500 or more individuals or fewer than 500 individuals. If a breach of unsecured PHI affects 500 or more individuals, a covered entity must notify the HHS Secretary of the breach without "unreasonable delay" and in no case later than 60 calendar days from discovery of the breach. In other words, any CIRCIA Report could be seen as acknowledgment of a data breach under HIPAA, and the reporting obligations timeline under HIPAA would begin.

[13] 45 C.F.R. § 164.408

Hospitals and healthcare systems would then be forced to balance obligations and differing timelines under two regulatory regimes – CIRCIA and HIPAA.

CISA is specifically proposing that: "For the fourth prong, a reasonable belief that unauthorized access was caused by a third-party provider or a supply chain compromise would be sufficient to trigger a reporting obligation, even if the cause of the cyber incident was not yet confirmed." **This proposal puts the burden of "reasonable belief" and the legal requirement solely on the hospital or healthcare provider that they must report an unconfirmed cyber incident caused by a third-party.**

Crucially, there are many third-parties in the healthcare ecosystem that our members contract with who would not be considered "covered entities" under this proposal, and therefore, would not be obligated to share or disclose that there had been a substantial cyber incident – or any cyber incident at all. The subjective nature of "reasonable belief" could potentially be exploited by third-parties, allowing individuals or organizations – covered entities or not – to justify their actions, or inactions. Additionally, should there be a substantial cyber incident on a third-party that is widely used in the HPH Sector, multiple providers could be impacted, resulting in multiple reports required to CISA.

CISA states that: "Timely reporting is of the essence for CISA to be able to quickly analyze incident reports, identify trends, and provide early warnings to other entities before they can become victims." **We agree that timely reporting will be critical to allow for CISA to provide early warnings to other entities before they can become victims, the onerous being placed solely on our members as covered entities, rather than third-parties who may or may not be covered entities, is extremely short-sighted. Additionally, 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 cyberattacks.**

CIRCIA Reports

CISA is proposing to include in the regulation a definition of the term CIRCIA Report. CIRCIA requires a covered entity to submit (either directly or through a third party) a report to CISA when it reasonably believes a covered cyber incident occurred, makes a ransom payment, or experiences one of a number of circumstances that requires the covered entity to update or supplement a previously submitted Covered Cyber Incident Report.[14] These reports are called Covered Cyber Incident Reports, Ransom Payment Reports, and Supplemental Reports, respectively.

CIRCIA additionally allows covered entities that make a ransom payment associated with a covered cyber incident to submit a single report to satisfy both the covered cyber incident and ransom payment reporting requirements.[15] CISA is proposing to call this joint submission a Joint Covered Cyber Incident and Ransom Payment Report. Additionally, CISA is proposing a term, CIRCIA Report, to be an umbrella term that encompasses all four types of covered entity reports collectively.

Our members – hospitals and health care systems – are already required to comply with a myriad of both state and federal cyber, security, and privacy data breach reporting

[14] 6 U.S.C. 681b(a)(1)-(3)
[15] 6 U.S.C. 681b(a)(5)(A)

requirements. These include federal authorities and requirements under the HIPAA[16] (including amendments to HIPAA made under the Health Information Technology for Economic and Clinical Health (HITECH Act)[10] regulations. Specifically, the HIPAA Breach Notification Rule,[17] as well as the HITECH Act's additional data breach reporting requirements to HHS' OCR,[18] as well as the FTC's Health Breach Notification Rule.[19]

Additionally, the Cybersecurity Information Sharing Act of 2015[20] marked a significant milestone by authorizing healthcare information threat sharing in certain situations. Nevertheless, healthcare organizations remain hesitant, fearing violations of HIPAA regulations and substantial reputational damage. Despite the potential reputational harm from a HIPAA breach, it is crucial for providers to share threat information to prevent 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 should be avoided.**

CISA states in the proposed rule:

> *Unfortunately, entities within [the HPH] sector routinely experience cyber incidents, with U.S. healthcare entities experiencing the seventh most cyber incidents of any industry in 2022. Many entities within the sector currently are required to report certain cyber incidents to HHS under the HIPAA Breach Notification Rule[21] and to the Federal Trade Commission under the HITECH Act Health Breach Notification Rule[22]; however, those requirements are generally focused solely on data breaches and do not require reporting of other types of cyber incidents that do not involve unauthorized acquisition of or access to personal health information.*

In 2023, OCR reported a 239 percent increase in hacking-related data breaches between January 1, 2018, and September 30, 2023, and a 278 percent increase in ransomware attacks over the same period. In 2019, hacking accounted for 49 percent of all reported breaches. In 2023, 79.7 percent of data breaches were due to hacking incidents.[23] Even HHS cited[24] a cohort study which concluded that ransomware attacks targeting HDOs doubled from 2016 to 2021. Hospitals and healthcare systems are among the entities within the HPH sector that are required to report certain cyber incidents to HHS – and we agree with CISA that "these requirements are generally focused solely on data breaches." **However, the vast majority of data breaches would also now fall under the definition of a "substantial cyber incident" as proposed.**

In our response to CISA's RFI, CHIME and AEHIS urged significant consideration and clarification in this proposed rule regarding the intersection and existing federal and state laws, regulations, and oversight. **We strongly recommended that the DHS and CISA coordinate with other**

[16] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191. https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996.
[17] Breach Notification Rule. (2021, June 28). HHS.gov. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[18] Breach Notification for Unsecured Protected Health Information. 74 FR 42739 and 74 FR 42767, Aug. 24, 2009. https://www.federalregister.gov/documents/2009/08/24/E9-20169/breach-notification-for-unsecured-protected-health-information
[19] Federal Trade Commission's Health Breach Notification Rule, 16 C.F.R. Part 318
[20] Pub. L. No. 114-113
[21] 45 CFR 164.400-414
[22] 16 CFR 318
[23] *Healthcare Data Breach Statistics*. (2024, May 23). The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/
[24] *2022 Healthcare Cybersecurity Year in Review, And A 2023 Look-Ahead*. https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

federal agencies with existing jurisdiction – including HHS, OCR, and the FTC – to minimize duplicative cyber incident reporting requirements to the greatest extent possible.

To reduce the burden on hospitals and healthcare systems, we strongly encouraged CISA to align with and leverage existing federal cyber incident and data breach reporting requirements for consistency. Reputational harm and higher information technology labor investment due to the remediation of data breaches is already an added cost to the impacted hospital and/or healthcare system.[25] **CHIME and AEHIS are disappointed that while we previously encouraged CISA to implement the reporting exemption for covered entities that submit cyber incident reports with substantially similar information to other Federal departments and agencies, within a substantially similar timeframe – they have not proposed to do so.**

Additionally, CIRCIA does not preempt state data breach notification laws, and it is unclear if CISA will engage state entities to harmonize CIRCIA reporting requirements with existing state laws. We are aware of existing state laws which would further complicate and burden our members without action from CISA. For example, Utah's recently enacted "The Protection of Personal Information Act", found at Utah Code 13-44-101, et seq., requires any non-government entity which conducts business in the State of Utah to prevent the unlawful use or disclosure of personal information collected by the organization.

> *If an organization that owns or maintains personal information of a Utah resident becomes aware of a breach of system security, that company must conduct an investigation to determine if the personal information has been or will be misused. If the investigation indicates that the misuse has occurred or is likely to occur, the organization must notify every affected Utah resident. If the misuse relates to 500 or more Utah residents, the organization must also provide notification to the Utah Attorney General's Office and the Utah Cyber Center.*[26]

"All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have laws requiring private businesses […] to notify individuals of security breaches of information involving personally identifiable information. Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data or information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information)."[27]

Further, "at least 40 states, Guam, Puerto Rico and Washington, D.C., introduced or considered more than 500 bills or resolutions that deal significantly with cybersecurity. Thirty-nine states, Puerto Rico, and Washington, D.C., enacted at least 130 bills and adopted at least 10 resolutions in 2023."[28] **Consequently, it will be incumbent upon CISA to proactively – and on an ongoing basis – engage with state entities to ensure harmonization, to the greatest extent possible, of the CIRCIA reporting requirements with existing state laws.**

---

[25] Lee J, Kim H, Choi SJ. Do hospital data breaches affect health information technology investment? *DIGITAL HEALTH*. 2024;10. doi:10.1177/20552076231224164

[26] *Report a breach · Cyber Center*. (n.d.). https://cybercenter.utah.gov/Report-a-Breach/

[27] *Security Breach Notification Laws*. (2023, October 12). https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

[28] *Cybersecurity 2023 Legislation*. (2023, October 12). https://www.ncsl.org/technology-and-communication/cybersecurity-2023-legislation

Covered Cyber Incident Report

CISA is proposing to include in the regulation a definition of the term Covered Cyber Incident Report. CIRCIA requires a covered entity that experiences a covered cyber incident to report that incident to CISA.[29] CISA is proposing to refer to this type of report as a Covered Cyber Incident Report and to define that term to mean a submission made by a covered entity or a third party on behalf of a covered entity to report a covered cyber incident. CISA is further proposing that a Covered Cyber Incident Report also includes any additional, optional information submitted as part of a Covered Cyber Incident Report. **CHIME and AEHIS broadly support this proposed approach. However, our concerns regarding the proposed Covered Cyber Incident Report Specific Content are detailed further in this letter.**

Supplemental Report, Meaning of "Substantial New or Different Information", and Meaning of "Promptly"

CISA is proposing to include in the regulation a definition of the term Supplemental Report. CIRCIA requires a covered entity to promptly submit an update or supplement to a previously submitted Covered Cyber Incident Report under certain circumstances.[30] CISA is proposing to refer to this type of report as a Supplemental Report. CISA is proposing that the term Supplemental Report be used to describe a submission made by a covered entity or a third party on behalf of a covered entity to update or supplement a previously submitted Covered Cyber Incident Report or to report a ransom payment made by the covered entity after submitting a Covered Cyber Incident Report as required. CISA is further proposing that a Supplemental Report also include any additional, optional information submitted as part of a Supplemental Report.

CISA states: "CIRCIA requires a covered entity to promptly submit an update or supplement to a previously submitted Covered Cyber Incident Report under certain circumstances. 6 U.S.C. 681b(a)(3)."

However, CIRCIA also states:

> *"Deadlines and criteria for submitting supplemental reports to the Agency required under subsection (a)(3), which shall—*
>
> *(A) be established by the Director in consultation with the Council;*
> *(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable;*
> *(C) balance the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations; and*
> *(D) provide a clear description of what constitutes substantial new or different information."*[31]

As required under § 681b(7)(B), CHIME and AEHIS respectfully request that CISA follow the letter – and intent – of the law and "consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also

[29] 6 U.S.C. 681b(a)(1)
[30] 6 U.S.C. 681b(a)(3)
[31] 6 U.S.C. § 681b(7)

be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable."

This would include allowing for a delay in reporting under CIRCIA in instances where proposed covered entities as defined under the HPH Sector as hospitals and CAHs are already working with law enforcement. For example, HIPAA[32] 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 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.[33]

The HIPAA Privacy Rule also permits a covered entity to disclose PHI to public officials who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism[34] 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.[35] **If CISA promulgates final 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. 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.**

Organizations that involved law enforcement saw significant time and cost savings when they were victims of ransomware. A report found that ransomware victims that opted to involve law enforcement to help contain a ransomware breach experienced a less costly breach overall – by nearly 10 percent. Additionally, the total time to identify and contain a ransomware breach was 11.4 percent (33 days) shorter with law enforcement involvement, at 273 days in total compared to 306 days. The mean time to contain a ransomware breach was 63 days shorter – nearly 24 percent – with law enforcement involvement. The report states: "It's clear that involving law enforcement can help reduce the cost and duration of a ransomware breach."[2]

This clearly underscores the crucial importance of collaborative efforts between hospitals, healthcare systems, and law enforcement – especially their partners in local Federal Bureau of Investigation (FBI) offices – to enhance cybersecurity and protect public health. Our members believe that these invaluable, existing partnerships should not be hindered by the final rule.

Additionally, while CISA is proposing to include as required content in CIRCIA Reports information on a covered entity's notification or other form of engagement with law enforcement agencies – there is little information provided or proposals offered as to how CISA will share data with law enforcement agencies, such as the FBI, or how they expect law enforcement to share information with CISA. **Consistent with Congressional intent – we respectfully request that CISA offer clarity in the final rule such that covered entities will not have to report the same incident**

---

[32] *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/for-professionals/faq/397/does-hipaa-permit-covered-entities-to-disclose-information-to-officials-responding-to-public-health-emergencies/index.html

[33] 45 CFR 164.512(b))

[34] 45 CFR 164.512(j))

[35] 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)).

multiple times to multiple agencies. CISA can significantly reduce redundancy, burden, and streamline the reporting process for covered entities by enhancing collaboration and coordination with other federal agencies and law enforcement.

Furthermore, as required under § 681b(7)(C), regarding deadlines and criteria for submitting supplemental reports to CISA – to "*balance the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations,"* CHIME and AEHIS strongly believe that patient safety in hospitals and healthcare systems means not just ensuring access to care – but ensuring that patient safety is not jeopardized. Cyberattacks targeting hospitals are considered "threat-to-life crimes" because disruption of patient care potentially has severe consequences on patient well-being and may lead to impaired health outcomes and increased mortality.[36]

Ransomware attacks are increasingly targeting our nation's hospitals and healthcare systems – and when successful, create disconcerting disruption.[21] One study stated that "the most notable effect of the ransomware attacks was the loss of technology availability as a direct result of the attack or as a preventive measure taken by IT staff." This study further found that: "In addition, the ransomware attacks "caused massive delays" in patient care, and providers worried that these delays led to worse outcomes."

While CHIME and AEHIS appreciate that CISA is proposing to allow for supplemental reporting after a substantial cyber incident – which we supported in our response to the RFI – we have significant concerns. These concerns are specifically related to the timing of the submission of supplemental reports, as well as the definition of "substantial new or different information" as proposed.

CISA is proposing to interpret "substantial new or different information" as meaning information that (1) is responsive to a required data field in a Covered Cyber Incident Report that the covered entity was unable to substantively answer at the time of submission of that report or any Supplemental Report related to that incident, or (2) shows that a previously submitted Covered Cyber Incident Report or Supplemental Report is materially incorrect or incomplete in some manner. CISA states: "Together, these two provisions will help ensure that a covered entity has provided to CISA all required information related to a covered cyber incident in a timely fashion and that any material inaccuracies in a previously submitted Covered Cyber Incident Report or Supplemental Report are promptly corrected."

CISA is further proposing to use the statutory language contained in 6 U.S.C. 681b(a)(3) verbatim in the regulation to identify the timeframe and associated trigger for providing Supplemental Reports to CISA. CIRCIA requires Supplemental Reports to be submitted "promptly" upon the occurrence of either of the two identified triggering events. "***CISA interprets "promptly" to generally mean what it means colloquially, i.e., without delay or as soon as possible*** [emphasis added]."

Under 6 U.S.C. 681b(a)(3), a covered entity that has previously submitted a Covered Cyber Incident Report must "promptly" submit to CISA an update or supplement to that report if either: (a) "substantial new or different information becomes available"; or (b) "the covered entity makes a ransom payment after submitting a covered cyber incident report." **CHIME and AEHIS are**

[36] Van Boven, L. S., Kusters, R. W., Tin, D., Van Osch, F. H., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C., & Barten, D. G. (2024). Hacking Acute Care: A qualitative study on the health care impacts of ransomware attacks against hospitals. *Annals of Emergency Medicine*, *83*(1), 46-56. https://doi.org/10.1016/j.annemergmed.2023.04.025

extremely concerned about CISA's interpretation of the word "promptly" in the proposed rule.

Given these concerns, it is imperative that CISA provides clear and practical guidance on the interpretation and implementation of "promptly" to ensure that covered entities can comply effectively without undue burden. This clarity is crucial to maintaining the balance between timely reporting and the operational realities faced by hospitals and healthcare systems, ultimately enhancing the overall cybersecurity posture and resilience of the sector.

If, as proposed, hospitals and healthcare systems are to provide detailed and numerous reports during, throughout, and after a substantial cyber incident, our members believe strongly that the supplemental reporting and timing of "without delay or as soon as possible" as proposed will mean that ensuring compliance with these reporting requirements could be prioritized over patient safety. As hospitals and "healthcare systems become increasingly reliant on digital systems to deliver care, healthcare organizations' readiness to manage critical infrastructure failure/breach is crucial for the continuity of care and patient safety."[37]

Further, there have been studies which suggest that cyberattacks on hospitals and healthcare systems are associated with greater disruptions to regional hospitals and should be treated as disasters, necessitating coordinated planning and response efforts.[38] In other words, a cyberattack on one hospital can have a ripple effect on surrounding hospitals – "hospitals adjacent to health care delivery organizations affected by ransomware attacks may see increases in patient census and may experience resource constraints affecting time-sensitive care for conditions such as acute stroke."[23]

When a hospital experiences a cyberattack, it is not an isolated incident but a critical event that can have far-reaching repercussions across the healthcare ecosystem. Cyberattacks on hospitals can disrupt essential services, compromising patient care and safety. The interconnected nature of healthcare facilities through shared networks, electronic health record (EHR) systems, and collaborative treatment efforts means that a breach in one institution can propagate risks to others. This can lead to a cascade of operational disruptions, delaying treatments, compromising data integrity, and overwhelming neighboring hospitals with increased patient loads. Consequently, the impact of such an attack can erode trust in the healthcare system, increase operational costs, and ultimately endanger patient lives.

For the reasons outlined above, given the complexities and significant impact a cyberattack can have on hospitals and health systems, CISA's interpretation of the word "promptly" to mean "without delay or as soon as possible" is extremely concerning. If finalized as proposed, it will codify a definition that is loose enough for hospitals and healthcare systems – even those using their reasonable belief, best faith judgment, and all resources and abilities available to them to be in compliance – to potentially be subject to later punishment. Further, it leaves gray areas for every HDO's legal and compliance teams to over and under interpret what is considered "as soon as possible."

---

[37] Abbou B, Kessel B, Ben Natan M, Gabbay-Benziv R, Dahan Shriki D, Ophir A, Goldschmid N, Klein A, Roguin A, Dudkiewicz M. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Front Digit Health. 2024 Feb 16;6:1321485. doi: 10.3389/fdgth.2024.1321485. PMID: 38433989; PMCID: PMC10904636.
[38] Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., Hemmen, T. M., Clay, B. J., & Longhurst, C. A. (2023). Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Network Open*, *6*(5), e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270

Additionally, hospitals and healthcare systems face unique challenges during cybersecurity incidents – including "difficulty predicting which facilities are at highest risk due to a lack of geographic association and institutional precedent, rapid spread across large distances within a hospital network affecting multiple facilities simultaneously, and protracted operational downtimes approaching weeks to months."[23] After a cyberattack, hospitals must go on downtime; the average downtime for hospitals in 2022 was 24 days with an average cost of $10 million – compromising access and resources for medical services.[39]

"While all hospitals undergo intermittent downtime, these typically happen with some warning and are relatively brief with a known timeframe. However, cyberattacks occur suddenly, with unique features including multiple systems simultaneously impacted and prolonged downtimes." Furthermore, because of "the unique nature of cyberattacks, an all-hazards approach that is typically used in disaster response is unlikely to suffice. **Cyberattacks occur at the speed of the Internet without warning, require specialists in information security (IS) and greatly compromise the existing clinical flow." [40] CHIME and AEHIS members believe strongly that cybersecurity is patient safety, and regulatory requirements should not jeopardize their core mission of care.**

Therefore, we strongly recommended that hospitals be allowed a reasonable, expected reporting cadence – when and if – "substantial new or different information" becomes available. For example, a balanced cadence for hospitals and health systems to submit a supplemental report with any "substantial new or different" information if it becomes available would be either every 72 hours, or ideally, five business days.

This consistency will ensure that providers can appropriately prioritize and triage patients during the impacted window while still complying with reporting mandates. Moreover, careful consideration should be given to what and when information is required to balance the urgency of patient care and recovery from an incident with regulatory compliance. There are other potential benefits, including reducing the burden on HDOs, to setting a regular supplemental reporting cadence – rather than "as soon as possible."

Firstly, CISA is going to be consistently receiving the most accurate and up-to-date information in a reasonable timeframe. Additionally, the number of reports that CISA will need to sort, compile, and disseminate will dramatically decrease. During and after a cyberattack, there may be "unknowns" in the initial Covered Cyber Incident Report – and hospitals and healthcare systems may have suspected an exploited vulnerability. However, to avoid potential disinformation being shared, until it is verified, a regular supplemental reporting cadence rather than "as soon as possible" ensures that accurate and reliable information reaches CISA in a timely manner.

Therefore, we are recommending that hospitals and healthcare systems be required to submit supplemental reports every 72 hours at minimum, or every five business days. This reporting cadence would be required only when and if substantial new or different information becomes available. CHIME and AEHIS strongly believe that this approach strikes a balance between patient care, HDO recovery, and regulatory compliance – which will benefit both our members and CISA.

---

[39] Gates L. Cyber Attacks on Interoperable Electronic Health Records: A Clear and Present Danger. Mo Med. 2024 Jan-Feb;121(1):6-9. PMID: 38404433; PMCID: PMC10887471.

[40] Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. (2023). A National survey of Hospital Cyber Attack Emergency Operation Preparedness. *Disaster Medicine and Public Health Preparedness*, *17*. https://doi.org/10.1017/dmp.2022.283

Meaning of "Concluded" and "Fully Mitigated and Resolved"

A covered entity's supplemental reporting requirements remain in effect until the covered entity notifies CISA "that the covered cyber incident at issue has concluded and has been fully mitigated and resolved."[41] CISA states that:

> *Although the point at which an incident is concluded and fully mitigated and resolved may vary based on the specific facts of the incident, reaching the following milestones is a good indication that an incident has been concluded and fully mitigated and resolved: (1) the entity has completed an investigation of the incident, gathered all necessary information, and documented all relevant aspects of the incident; and (2) the entity has completed steps required to address the root cause of the incident (e.g., completed any necessary containment and eradication actions; identified and mitigated all exploited vulnerabilities; removed any unauthorized access).*

While CHIME and AEHIS members generally agree with this approach, we wish to point out that there is a difference between "mitigated" and "resolved." Mitigation refers to the implementation of measures that reduce the risk or impact of a vulnerability. The issue may still exist, but its potential to cause harm is significantly lessened. Resolved refers to the complete fixing or elimination of a vulnerability; the issue is fully addressed, and the security gap is closed.

CISA is proposing: "For an incident to be concluded and fully mitigated and resolved, a covered entity should have a good-faith belief that further investigation would not uncover any substantial new or different information about the covered cyber incident." **CHIME and AEHIS believe that rephrasing this proposal, for clarity purposes and to emphasize the important distinction between "mitigated" and "resolved" to state: "*For a substantial cyber incident to be concluded, a covered entity* should have a good-faith belief […]."**

CISA does not believe that all damage caused by the incident must have been fully addressed and remediated for an incident to be considered concluded and fully mitigated and resolved. **CHIME and AEHIS members appreciate this approach, as there are cyber incidents where a hospital or healthcare system may never get data back, and/or there will be set/s of data that are not recoverable.**

Proposed Size-Based Criteria & Proposed Sector-Based Applicability Criteria

CISA is proposing that the description of covered entity include any entity in a critical infrastructure sector that exceeds the small business size standard specified by the applicable North American Industry Classification System Code in the Small Business Administration (SBA) Size Standards.[42] These standards "define whether a business is small and, thus, eligible for Government programs and preferences reserved for 'small business' concerns." While designed in large part for determining eligibility to participate in certain Federal government contracts, procurements, grants, and other similar purposes, the Small Business Size Regulations indicate that the SBA Size Standards are for general use by Federal departments and agencies promulgating regulations that include size criteria. If a Federal department or agency wants to use different size criteria, it is required to consult with the SBA in writing during the rulemaking process and explain why the SBA's existing size standards would not satisfy program

[41] 6 U.S.C. 681b(a)(3)
[42] 13 CFR part 121

requirements. CISA believes the SBA Size Standards are well-suited for use as the size-based threshold aspect of the CIRCIA Applicability section.

CISA is also proposing to include as part of the description of covered entity in the Applicability section a series of criteria that are based on characteristics typically associated with entities in one or more specific critical infrastructure sectors or subsectors. Specifically, CISA is proposing to include in the scope of covered entity any entity that meets one or more of a set of specified sector-based criteria, each of which is described in the proposed rule. CISA states: "These criteria apply regardless of the specific critical infrastructure sector of which the entity considers itself to be part." Additionally, CISA is specifically interested in receiving comments on:

> *1) The scope of entities that would and would not be considered covered entities based on the three criteria proposed by CISA, whether the scoping is appropriate, and what, if any, specific refinements should CISA consider related to any of the criteria; and*
> *2) The proposal to forgo including specific criteria focused on health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities.*

Our detailed comments on the HPH Sector-based proposals as they relate to our members – hospitals and healthcare systems – are detailed below. "CISA recognizes that entity size and other characteristics can be dynamic, and whether an entity meets the size-based threshold or other criteria for being a covered entity may vary depending on when the entity assesses if they meet the criteria set forth in § 226.2." **Therefore, rather than allowing entities to "self-assess" if they meet the criteria CISA is proposing, CHIME and AEHIS members strongly encourage CISA to include specific HPH Sector-based criteria focused on health insurance companies, third-party administrators (TPAs) of health plans, and healthcare clearinghouses. None of these third-parties are listed under the SBA's table of small business size standards "Sector 62 – Health Care and Social Assistance." Rather, some – including "Direct Health and Medical Insurance Carriers," are listed under "Sector 52 – Finance and Insurance." We are extremely concerned that if these third-parties are not explicitly "carved-into" the HPH Sector-based criteria, that they may simply self-assess that they do not meet the proposed criteria, and are not subject to CIRCIA.**

CHIME and AEHIS understand that CISA is proposing additional, sector-based criteria for a variety of reasons. As CISA states: "As noted in the discussion regarding the size-based criterion, an entity's size does not necessarily reflect its criticality. Some entities in a critical infrastructure sector that fall below the proposed size-based thresholds own or operate systems or assets that would be likely to meet the definition of critical infrastructure set forth by 42 U.S.C. 5195c(e)." **CHIME and AEHIS broadly agree with these assertions and they are why we are urging CISA to include health plans, health insurance companies, TPAs of health plans, and healthcare clearinghouses under the HPH Sector-based criteria.**

Amidst an increasingly complex cybersecurity landscape, our members strive, and sometimes struggle, to manage third-party risk effectively. Hospitals and healthcare systems are forced to be dependent on third-party services – and often have contracts with them numbering in the thousands – which means that any disruption or failure on their part can directly affect our members' operations. **When a third-party breach occurs, business partners or third-party software that support clinical or business operations become infected, in turn infecting networked clinical and business operations of the healthcare entity.**

Furthermore, as our members can attest often happens, when third-parties resist signing HIPAA BAAs or accepting appropriate liability levels, the HDO faces the legal risks. Without clear agreements, responsibilities and liabilities become ambiguous. CISA states, "***their*** [emphasis added] devices, systems, and networks"; however, we must reiterate that hospitals and healthcare systems do not manufacture medical devices, nor are they responsible for running other companies and ensuring they have implemented appropriate cybersecurity measures, such as healthcare clearinghouses.

CHIME and AEHIS members have been victims due to cyberattacks on third-party services or breaches affecting their vendors and contractors. There is no greater example of the devastating impact this can have on healthcare than the unprecedented cyberattack on Change Healthcare this year. On February 21, 2024, Change Healthcare, a unit of UHG, discovered a threat actor gained access to one of their environments. A Russia-affiliated ransomware group known as AlphV or BlackCat claimed responsibility. According to UHG CEO Andrew Witty's Congressional testimony, "criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, an application used to enable remote access to desktops. The portal did not have multi-factor authentication. Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data. Ransomware was deployed nine days later." In Questions for the Record (QFR) submitted to the Senate Finance Committee, UHG stated that "given the "ongoing nature and complexity of the Company's data review" it will "take additional analysis before enough information will be available to identify affected customers and individuals." However, during a Congressional hearing Witty estimated that a third of all Americans data could be impacted.

This is the most massive cyberattack on our sector to date – much larger than the WannaCry event experienced several years ago – and it wreaked unprecedented havoc on the entire healthcare ecosystem given the data clearinghouse and transaction hub role that Change provides at national scale. The interruption to patient care as well as the financial impact on our members has been devastating. Providers affected by this breach are so numerous that a specific number is not readily available.

A report[43] from the Health Information Sharing and Analysis Center (Health-ISAC) – the operational defense collective of the health sector – surveyed its members asking them to rank order the Top 5 "greatest cybersecurity concerns" facing their organizations from 2023 to 2024, and third-party risk replaced compromised credentials in the top five cyber threats for 2024. Further, third-party vendors often handle sensitive patient data, and thus – any security breach on them can lead to data exposure, privacy violations, and legal consequences. These incidents erode patient trust and can damage the reputation of hospitals and healthcare systems.

CISA states: "One of the main purposes of this regulatory program authorized by CIRCIA is to enhance the security and resiliency of critical infrastructure, and therefore receiving Covered Cyber Incident Reports and Ransom Payment Reports from as many entities that own or operate critical infrastructure as possible is imperative to meet this directive." **If CISA is to achieve this purpose – and truly enhance the security and resiliency of critical infrastructure – CHIME and AEHIS believe that the final rule must include, at minimum, the third-parties listed above. Health plans, health insurance companies, TPAs of health plans, and**

[43] Executive Summary for CISOs: Current and Emerging Healthcare Cyber Threat Landscape. (2024). In *https://h-isac.org/current-and-emerging-healthcare-cyber-threat-landscape-executive-summary-for-cisos/*. https://h-isac.org/current-and-emerging-healthcare-cyber-threat-landscape-executive-summary-for-cisos/

clearinghouses hold vast quantities of patient data and are integral partners in the healthcare system, as evidenced by the Change Healthcare attack.

Healthcare and Public Health (HPH) Sector Proposals

CISA is proposing to include in the description of covered entity multiple sector-based criteria related to the HPH Sector. The first criterion CISA proposes related to this sector will mean that certain entities providing direct patient care will be considered covered entities. CISA is proposing requiring reporting from larger hospitals (i.e., those with more than 100 beds) and CAHs. Specifically, CISA is proposing including in the description of covered entity any entity that owns or operates (1) a hospital, as defined by 42 U.S.C. 1395x(e), with 100 or more beds, or (2) a CAH, as defined by 42 U.S.C. 1395x(mm)(1). CISA believes it is "worthwhile to focus on larger hospitals for required reporting, as they are more likely than smaller hospitals to experience substantial impacts if they fall victim to a covered cyber incident given their size and the correspondingly greater number of patients they are caring for on any given day."

CISA also states: "Additionally, focusing on larger hospitals is supported by much of the same rationale behind CISA's decision to propose an overall size-based criterion based on the SBA small business size standards in the Applicability section (***e.g., larger hospitals are more likely to have in-house or access to cyber expertise; larger hospitals are likely to be better equipped to simultaneously respond to and report a cyber incident)*** [emphasis added]."

There are 6,120 hospitals in the U.S.; of these, there are 5,129 U.S. community hospitals, 2,987 nongovernment not-for-profit community hospitals, 1,219 for-profit hospitals, and 923 state and local government community hospitals. There are 207 Federal Government hospitals, and 125 that fall under "other."[44] In other words, 58 percent of community hospitals are non-government and not-for-profit, 24 percent are investor-owned and for-profit, and 18 percent are state and local government owned. The number of staffed beds in all U.S. hospitals is 916,752 and the number of staffed beds in community hospitals is 784,112.

According to HHS, in 2022 – not including CAHs – "almost half of hospitals are non-profit and they are larger hospitals on average, with a mean bed size of 209 (vs. 107 for for-profit and 175 for government hospitals)."[45] The SBA's NAICS Code, 622110 for the NAICS Industry Description "General Medical and Surgical Hospitals" has a size standard in millions of dollars of $47 million. CISA's rationale to focus on "larger hospitals" being supported by the same rationale for proposing an overall size-based criterion based on the SBA small business size standards is inherently flawed. Firstly, in order to meet the SBA's numerical standards for small, the business must be a for-profit business.[46] Nearly half of the hospitals in the U.S. are non-profit entities. The Centers for Medicare & Medicaid Services (CMS), per the Hospital Provider Cost Report, defines the "bed size" of a hospital as the "number of beds available for use by patients at the end of the cost reporting period. A bed means an adult bed, pediatric bed, birthing room, or newborn ICU bed (excluding newborn bassinets) maintained in a patient care area for lodging patients in

[44] *Fast facts on U.S. hospitals, 2024 | AHA*. (2024, May 10). American Hospital Association. https://www.aha.org/statistics/fast-facts-us-hospitals

[45] Welch, W. P., Xu, L., De Lew, N., Sommers, B. D., & aspe.hhs.gov. (2023). *Ownership of Hospitals: An Analysis of Newly-Released Federal data & a Method for Assessing common Owners*. https://aspe.hhs.gov/sites/default/files/documents/582de65f285646af741e14f82b6df1f6/hospital-ownership-data-brief.pdf

[46] U. S. Small Business Administration. (2022). Table of small business size standards matched to North American Industry Classification System codes. In *U. S. Small Business Administration*.

acute, long term, or domiciliary areas of the hospital."[47] Further, the Agency for Healthcare Research and Quality (AHRQ) defines hospital bed size categories as: "Bedsize categories are based on hospital beds, and are specific to the hospital's location and teaching status. Bedsize assesses the number of short-term acute care beds set up and staffed in a hospital."[48]

CMS also permits, under the Social Security Act,[49] certain small, rural hospitals to enter into a swing bed agreement, under which the hospital can use its beds, as needed, to provide either acute or skilled nursing facility (SNF) care. As defined in the regulations, "a swing bed hospital is a hospital or critical access hospital (CAH) participating in Medicare that has CMS approval to provide post-hospital skilled-nursing facility (SNF) care and meets certain requirements. Medicare Part A (the hospital insurance program) covers post-hospital extended care services furnished in a swing bed hospital." Swing bed hospitals and CAHs are invaluable to their communities and the patients they care for, and it is unclear if swing beds would be counted for in the number of beds as proposed.

During the COVID-19 Public Health Emergency (PHE), hospitals were required to report on "capacity" – which included "all hospital inpatient beds", defined as: "Total number of all staffed inpatient beds in the facility, that are currently set-up, staffed and able to be used for a patient within the reporting period. This includes all overflow, observation, and active surge/expansion beds used for inpatients. This includes ICU beds. Include any surge/hallway/overflow beds that are open for use for a patient, regardless of whether they are occupied or available."[50] There were also subsets of inpatient bed numbers to account for capacity.

Fundamentally, this shows that "number of beds" is not simple and can mean a variety of different definitions depending on the context and the specific requirements of the reporting body. This complexity underscores the inadequacy of using a single criterion, such as "hospitals with 100 beds or more," to determine hospital size or capacity. The different definitions by the HHS, SBA, and CMS illustrate that bed count alone does not provide a comprehensive picture of a hospital's operational scope or financial status. For instance, the HHS data highlights significant differences in average bed size across non-profit, for-profit, and government hospitals. The SBA's financial size standard further complicates matters by applying criteria that do not align with the non-profit status of nearly half the hospitals in the U.S. Additionally, CMS's varied definitions during the COVID-19 PHE further illustrate the challenges of using bed numbers as a singular metric. **These factors combined suggest that a more nuanced approach, considering multiple criteria beyond just bed count, is necessary to accurately characterize hospital size and capacity.**

While CISA is not generally proposing to require reporting from "smaller hospitals", they are proposing to require reporting from critical access hospitals (CAHs). As CISA notes, CAHs are facilities that have been certified by CMS as meeting certain criteria, including that they are located in a state that has established a Medicare rural hospital flexibility program, and that they are designated as a critical access hospital by the State in which they are located, among other

---

[47] *Centers for Medicare & Medicaid Services data*. (n.d.). https://data.cms.gov/resources/hospital-provider-cost-report-data-dictionary

[48] *Healthcare Cost and Utilization Project (HCUP) NIS notes*. (n.d.). https://hcup-us.ahrq.gov/db/vars/hosp_bedsize/nisnote.jsp

[49] Section 1888(e) of the Social Security Act (the Act)

[50] Centers for Disease Control and Prevention (CDC). (2023). *Guidance for hospitals and acute care facilities reporting of respiratory pathogen, bed capacity, and supply data to CDC's National Healthcare Safety Network (NHSN)*. https://www.hhs.gov/sites/default/files/covid-19-faqs-hospitals-hospital-laboratory-acute-care-facility-data-reporting.pdf

requirements. CISA is proposing "to include these in the reporting requirements as they typically are the only source of emergency medical care for individuals living within certain rural areas. As a result, a substantial cyber incident at a critical access hospital may have disproportionate impacts to its size given the limited alternative emergency healthcare options for individuals within its service area."

The Biden administration recently acknowledged the unique challenges CAHs face and recognized the critical role these hospitals play in the communities they serve, stating: "Healthcare-related cyber disruptions can be particularly disruptive to rural hospitals, which serve over 60 million Americans. Most rural hospitals are critical access hospitals, meaning they are located more than 35 miles from another hospital, which makes diversions of patients and staffing-intensive manual workarounds in response to attacks more difficult."[1]

Additionally, according to the National Rural Health Association (NRHA): "Rural health clinics, hospitals, and health care entities lack funding, personnel, and preparedness to prevent and respond to cyberattacks. […] Enhancing cybersecurity in rural health care settings requires a collaborative effort involving governments, health care organizations, technology providers, and cybersecurity experts. By allocating resources, improving infrastructure, providing education and training, fostering collaboration, and implementing appropriate regulations, policymakers can significantly reduce cybersecurity risks and protect the integrity of patient data in rural health care settings."[51]

While we agree with CISA that CAHs are often the only source of emergency medical care for individuals living within certain rural areas, CHIME and AEHIS believe that introducing additional regulatory burdens on rural hospitals could have an inadvertent and devastating impact on CAHs and the patients they serve. Rural hospitals already operate on thin financial margins and face unique challenges. The financial impact of cyberattacks have attributed to recent rural hospital closures,[52] and adding more regulatory requirements could exacerbate these financial pressures. Rural healthcare providers – especially CAHs – are often the only healthcare providers in their communities, and their closure can leave residents without access to essential medical services. **This outcome is contrary to protecting public health, as it could reduce the availability and accessibility of healthcare in rural areas.**

Additionally, compliance with new regulations often requires substantial investments in cybersecurity infrastructure and training, which rural hospitals may struggle to afford. Unlike their larger counterparts, rural hospitals often lack the financial resources and technical expertise needed to implement comprehensive cybersecurity measures. **This financial strain can divert funds away from critical healthcare services, undermining the hospital's ability to serve its patients and community effectively.**

Furthermore, the administrative burden of additional reporting and compliance requirements can overwhelm the limited staff of rural hospitals. Rural hospitals typically have smaller administrative teams, which means that new regulations can lead to significant operational disruptions. **This can result in slower response times to cyber incidents and decreased overall efficiency, making rural hospitals more vulnerable to attacks rather than more secure.**

---

[51] Hassell, M., & Niblock, J. (n.d.). *Cybersecurity: A path to increase rural health care preparedness*. https://www.ruralhealth.us/getmedia/ad0774a2-49b4-4f9a-b2c5-2edf0eaf6bcf/2024-NRHA-Cybersecurity-Rural-Health-policy-brief.pdf

[52] Reed, T. (2023, June 16). Hospitals could be one cyberattack away from closure. *Axios*. https://www.axios.com/2023/06/16/hospitals-cyberattack-away-closure

Cyberattacks can be especially catastrophic for CAHs, which often lack the resources to effectively prevent and address security threats and are frequently the sole healthcare providers for their communities. **Therefore, CHIME and AEHIS believe that absent additional funding and workforce assistance to CAHs, CISA's proposed scope to include them such that they would be considered covered entities in this rule – is not appropriate at this time. Imposing additional regulatory burdens on rural hospitals could inadvertently increase their financial and operational strain, leading to more closures and reduced access to healthcare – and importantly – it could divert resources away from patient care. These outcomes would be contrary to the intent of enhancing the cybersecurity posture of all hospitals and healthcare systems and protecting public health – highlighting the need for tailored, supportive measures that consider the unique challenges faced by rural healthcare providers.**

CISA is proposing to focus on hospitals, "as they routinely provide the most critical care of the various types of entities providing direct care to patients – 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." **CHIME and AEHIS strongly believe that due to the lives at potential risk, should a hospital or healthcare system 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.)**

CHIME and AEHIS members wish to reiterate that 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 HPH Sector only as strong as its weakest link, it is imperative that CISA prioritize assisting both smaller and also lesser resourced (i.e., safety-net) providers in fending off growing and sophisticated attacks aimed at stealing intellectual property, extorting ransoms, threatening patients by targeting them, and hindering their ability to deliver care overall.**

Manner, Form, and Content of Reports

Pursuant to 6 U.S.C. 681b(a)(6) of CIRCIA, covered entities must make CIRCIA Reports in the manner and form prescribed in the final rule. CIRCIA requires CISA to include procedures for submitting these reports in the final rule, including the manner and form thereof. CIRCIA gives CISA broad discretion in determining the manner and form for submission of CIRCIA Reports, although it requires[53] CISA to "include, at a minimum, a concise, user-friendly web-based form" as one manner for submission of required reports.

In this proposal, not only does CISA intend to offer a web-based form as a manner of submission of CIRCIA Reports, for several reasons CISA agrees with those commenters who suggested that an electronic, web-based form is the preferred manner for submission of CIRCIA Reports. **CHIME and AEHIS members broadly agree with this approach. However – we strongly believe that covered entities should be able to test the proposed web-based forms before the issuance of the final rule, for all four of the proposed "CIRCIA Reports."** As proposed, the term "CIRCIA Reports" encompasses the four types of covered entity reports collectively, Covered Cyber Incident Report, Ransom Payment Report, Joint Covered Cyber Incident and Ransom Payment Report, and Supplemental Report. **A critical aspect for CISA to consider is the ability**

[53] 6 U.S.C. 681b(c)(8)(A)

for covered entities to be able to test the CIRCIA Reports – in web-based form – before this rule is finalized.

Therefore, we strongly recommend that CISA implement a sandbox environment version of the web-based forms for each of the proposed CIRCIA Reports well in advance of deploying them for reporting purposes. By initially isolating the forms in a controlled environment – where they can be executed and tested safely without risking any of the overall systems and networks – both CISA and covered entities will benefit. Additionally, the sandbox forms would allow organizations to familiarize themselves with the forms, test their functionality, and help ensure seamless reporting when it is required. Waiting until an actual substantial cyber incident occurs to use the form is suboptimal, as it may lead to delays and potential errors during critical moments.

CISA states that "a web-based form is a cost-effective way to gather information from large numbers of submitters both simultaneously and over time. If designed properly, it allows for significant standardization of data (in both form and content) and tailoring of circumstance-specific questions using dynamic prompts and responses incorporating conditional logic filters and conditional or branching questions."

CHIME and AEHIS broadly agree; however, to ensure it is designed properly, it will be essential to create a sandbox environment where the form can be accessed and tested by covered entities. As our 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. They are able and willing to provide input on the forms and offer to serve as "beta-testers."

We reiterate that this sandbox should be made available well in advance of the issuance of the final rule and should remain accessible thereafter. The opportunity to practice using the forms in a non-incident setting is crucial; it allows organizations to familiarize themselves with their structure and functionality. This preparation ensures that when an actual substantial cybersecurity incident occurs, the reporting process is smooth and efficient, rather than compounded by unfamiliarity with the form/s.

CISA states that a "web-based form can also reduce the likelihood of human error during the data submission process in various ways." **Allowing a period for testing and adaptation is crucial to reduce the likelihood of error – as well as for the efficacy of the reporting process. It prevents the first use of the form from coinciding with the high-pressure situation of managing an ongoing cyber incident, thereby reducing the risk of errors and delays in reporting. Additionally, ensuring that covered entities have adequate time and resources to adapt to the new reporting requirements under CIRCIA will enhance and improve the overall effectiveness of the law.**

As CISA notes, a web-based form can reduce problems and errors for some of the data that they expect covered entities may often need to report, such as malware hashes or IP addresses, which typically are long strings of numbers and/or letters. CISA states: "A web-based form only requires the involvement of a single individual (i.e., the person entering the information into the form on behalf of the covered entity) and allows for that individual to review information after entry but prior to submission, greatly reducing the potential for such errors."

However, it is extremely unrealistic that in a real-life scenario, that any reporting of a substantial cyber incident – no matter the format – will only involve a "single individual." Any reporting will undoubtedly require the facilitation of communication between everyone ranging from c-suite executives, senior leadership, IT and technical teams, legal and compliance, and external stakeholders – such as cyber insurance carriers. **CHIME and AEHIS strongly believe that the best way to reduce the potential for reporting errors is to sandbox the forms and allow covered entities to practice using them.**

Additionally, we strongly recommend that any updates or modifications to the web-based forms be first released to the sandbox environment for a notice period. This proactive approach ensures that organizations can adapt their procedures and stay compliant with the evolving requirements. By providing advance notice, organizations can align their internal processes and train relevant personnel accordingly. **We share CISA's goals and wish to enhance incident response capabilities while minimizing disruptions during actual cyber incidents.**

CISA is proposing that, "by using drop-down menus, radio buttons, or other limited response options where feasible and appropriate, a web-based form reduces the likelihood of human error resulting from the submitter not understanding the types of responses a question is seeking or CISA not understanding a narrative answer provided by a submitter."

CISA also states that a "web-based form both allows for greater standardization of responses and does so in a machine-readable format, and, in doing so, it facilitates a number of activities that are much more challenging when data is submitted in other manners. These activities include automated triage of reports; rapid, large-scale trend analysis; timely information sharing; and long-term storage, many of which CISA is required by CIRCIA to perform."

CHIME and AEHIS members believe that encouraging entities to report their data using a standard protocol is appropriate to ensure consistency, interoperability, and enhanced data security. However, mandating this practice may not always be practical due to varying capacities and resources among different hospitals and healthcare systems. Therefore, while the adoption of standard reporting protocols should be strongly promoted, flexibility should be maintained to accommodate covered entities where it is currently infeasible.

Additionally, our members believe that data reporting requirements should be balanced, and CISA must minimize data reporting to only what information is absolutely necessary; minimal necessary data is a cybersecurity best practice. Adopting minimal data collection and retention practices as a cybersecurity standard is crucial for reducing risk, enhancing privacy, improving data management, preventing unauthorized access and misuse, mitigating insider threats, and simplifying incident response. Data should only be collected for a specific purpose, and only as much as needed to fulfill this given purpose.[54]

By adhering to this cybersecurity principle, both CISA and our members can better protect their systems and the sensitive information they handle. Further, by limiting data sharing to include only what is necessary helps to facilitate the spirit of CIRCIA – which is to reduce national cyber risk and threat information sharing in order to help avert and prevent cyberattacks.

[54] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

Covered Cyber Incident Report Specific Content

CISA is proposing requiring submission of information in specific categories of content in a Covered Cyber Incident Report. As noted in the individual content categories, CISA is proposing that some of the proposed data elements within the individual content categories are required while other proposed data elements are optional. CISA intends to ask for all the required information in an initial Covered Cyber Incident Report; however, CISA understands that a covered entity may not know all of the required information within the initial 72-hour reporting timeframe. Accordingly, answers of "unknown at this time" or something similar will be considered acceptable for certain questions in initial reporting.

CHIME and AEHIS appreciate the option to answer "unknown at this time" and the flexibility that this will offer our members. It is crucial to meticulously balance both the type and timing of information needed to effectively handle the urgency of patient care, and mitigation from a cyber incident with adherence to regulatory compliance. Hospitals and healthcare systems should only be required to report details after initial mitigation and response efforts – given their core mission is patient safety and care.

However, if CISA is to require "other information" in any of the CIRCIA Reports that is not already detailed in this proposed rule, it should remain optional unless and until it is proposed by CISA through a future notice-and-comment-rulemaking process in order for the public to provide feedback.

Vulnerabilities, Security Defenses, and TTPs

The second statutorily required block of content is focused on how the incident was carried out. Specifically, 6 U.S.C. 681b(c)(4)(B) requires covered entities to include in a Covered Cyber Incident Report "[w]here applicable, a description of the vulnerabilities exploited and security defenses in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident."

As stated in the proposed rule: "This information will enable CISA to carry out its core statutory responsibilities related to identifying and sharing information on cyber incident trends, TTPs, vulnerability exploitations, campaigns, and countermeasures that may be useful in preventing others from falling victim to similar incidents and preventing similar vulnerability classes in the future."

CISA is proposing to codify the need to submit information to address this statutory requirement in five consecutive regulatory subsections. Proposed § 226.8(d) would require "a description of the covered entity's security defenses in place, including but not limited to any controls or measures that resulted in the detection or mitigation of the incident."

CHIME and AEHIS members are extremely concerned about the definition proposed in § 226.8(d). Firstly, if hospitals and healthcare systems are required to define their entire security architecture, that is a tremendous amount of information to include in a report – which is simply not an efficient use of time or resources. Our members do not believe that CISA needs to know an entire description of an organization's security program – as it is not helpful to the rest of the sector, is potentially considered intellectual property (IP), and/or sensitive for the organization.

Furthermore – and extremely concerning – if the entire security architecture of a hospital or healthcare system is sent to CISA, it is the most target rich information for bad actors. Our members believe that the other proposed reporting requirements would be more than sufficient for CISA to share the necessary threat information with other covered entities.

The proposed language "including but not limited to" should be stricken from the final rule, and at minimum, changed to "only including" – so that § 226.8(d) reads "A description of the covered entity's security defenses in place, only including any controls or measures that resulted in the detection or mitigation of the incident."

Furthermore, CISA notes they are "likely to ask what, if any, security controls or control families (e.g., NIST Special Pub 800-171 controls; NIST Cybersecurity Framework measures; CISA Cybersecurity Performance Goal activities) the covered entity had in place on the compromised system, and, to the extent known, which controls or control families failed, were insufficient, or not implemented that may have been a factor in this incident." This information would be above and beyond sufficient for CISA to share information on cyber incident trends, eliminating the need for proposed § 226.8(d).

"CISA also is likely to include questions aimed at helping CISA understand how the covered entity identified the incident; what, if any, detection methods were used to discover the incident; and if the covered entity has identified the initially affected device(s)." We wish to reiterate that this information would provide CISA with a thorough "***[w]here applicable*** [emphasis added] description of the vulnerabilities exploited and security defenses in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident as required under 6 U.S.C. 681b(c)(4)(B). **CHIME and AEHIS members reiterate that CISA should not finalize "likely to include questions" in any of the CIRCIA Reports that are not already detailed in this proposed rule, unless they are optional. Any new questions should be proposed by CISA through a future notice-and-comment-rulemaking process in order for the public to provide meaningful input.**

<u>Data and Records Preservation Requirements</u>

Under CIRCIA, any covered entity that submits a CIRCIA Report must preserve data relevant to the reported covered cyber incident or ransom payment in accordance with procedures established in the final rule.[55] To implement this requirement, CISA is to include in the final rule, a clear description of the types of data that covered entities must preserve, the period of time for which the data must be preserved, and allowable uses, processes, and procedures.

CISA is proposing requiring covered entities to preserve a variety of data and records related to any covered cyber incidents or ransom payments reported to CISA in a CIRCIA Report. CISA is specifically proposing to require covered entities:

> *preserve data and records relating to communications between the covered entity and the threat actor; indicators of compromise; relevant log entries, memory captures, and forensic images; network information or traffic related to the cyber incident; the attack vector; system information that may help identify vulnerabilities that were exploited to perpetrate the incident; information on any exfiltrated data; data and records related to any ransom payment made; and any forensic or other reports about the cyber incident produced or procured by the covered entity.*

[55] 6 U.S.C. 681b(a)(4)

A covered entity that has any of the data or records listed above must preserve that data or records regardless of what format they are in, whether they are electronic or not, located onsite or offsite, found in the network or in the cloud, etc. A covered entity is not, however, required to create any data or records it does not already have in its possession based on this regulatory requirement. The requirement for a covered entity to preserve data or records applies only to the extent the entity already has created, or would be creating them, irrespective of CIRCIA.

For instance, rather than require covered entities retain all log entries or memory captures from the time of the incident in case any of them may have contained pertinent data, CISA is proposing to limit this to log entries, memory captures, or forensic images that the covered entity believes in good faith are relevant to the incident. Similarly, CISA is not proposing that a covered entity be required to preserve copies of all data that was exfiltrated during an incident, but rather simply proposes that a covered entity preserve information sufficient to understand what type of and how much data was exfiltrated.

CHIME and AEHIS members believe that the types of data that covered entities must preserve should only be data elements that were material to the conclusions for the methods and tactics used by the threat actors. The preservation of full forensic information and network traffic are extremely burdensome and costly for hospitals and healthcare systems.

CISA also has discretion in the period for Data and Records Preservation. And, as CISA notes, "this would not impact the government cost, as this is a cost borne by industry." CISA also estimates costs associated with Data and Records Preservation; stating that a covered entity would spend six hours per submission to collect, store, and maintain records in the first year of the preservation period. The cost of this provision is based on an hourly compensation rate of $35.19, which is the rate for Office and Administrative Support. Based on six hours per year, at $35.19 per hour, the annual labor cost of data and record preservation would be $211.12.

CHIME and AEHIS members strongly disagree with this estimation. The estimated allocated hours are extremely insufficient for the Data and Records Preservation requirements as proposed. Collection and preservation efforts must be integrated into incident response and investigation plans, which typically span days to weeks. The current estimate rate is also inadequate, and inaccurately estimated. These tasks will require specialized internal cybersecurity staff – not basic administrative support. Additionally, many organizations will need to hire external firms, which charge upwards of $300 per hour, to handle these complex investigations.

According to *A Cost Analysis of Healthcare Sector Data Breaches* from the Health Sector Cybersecurity Coordination Center (HC3), "Direct expenses include engaging forensic experts, outsourcing hotline support, and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates." Direct and indirect costs incurred by an organization are added up to calculate the cost of a data breach.[56] Furthermore, "both of these costs increased in the United States from 2017 to 2018 due to factors such as prioritizing speed of victim notifications over having a thorough and comprehensive understanding of the scope and impact of a data breach, compliance failures, the need for consultants and potential lawsuits which all contribute to these

[56] Health Sector Cybersecurity Coordination Center (HC3). (2019). *A cost analysis of healthcare sector data breaches*. https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf

costs." Finally, due to response and recovery activities as well as business opportunity costs and the potential loss of patients, data breaches are costly events for a healthcare organization.

Benefits

The primary purpose of CIRCIA is to help preserve national security, economic security, and public health and safety. "The provisions included in this proposed rule would support that purpose in a number of ways, providing several benefits." CISA states:

> *Over the last decade, the United States has seen an exponential increase in cyber incidents, with nation-states, criminal actors, and other malicious cyber threat actors targeting entities across all of the critical infrastructure sectors with ever-evolving tactics, techniques, and procedures. Addressing this growing, dynamic threat requires a better understanding of the threat and the vulnerabilities being exploited, and the timely sharing of that information with owners and operators of internet-connected information systems so that they can take steps to better secure themselves from potential cyber incidents.*

CISA further notes that: "CIRCIA would help the Federal government address this shortcoming by helping the Federal government understand the cyber threat landscape and enabling the timely sharing of information to enhance cyber resilience."

CHIME and AEHIS members are strongly supportive of the purpose of CIRCIA, as well as the above statements. Cybersecurity is a shared responsibility across the federal government, all of the critical infrastructure sectors, and within the HPH Sector, specifically. The HPH Sector is unfortunately being targeted by cybercriminals at the highest rates – with ransomware attacks steadily increasing, and nearly doubling in 2023 from the previous year. In the U.S., attacks against the healthcare sector have increased by 128 percent, with 258 victims in 2023 versus 113 in 2022.[57] The administration has further recognized that effective cybersecurity is critical to Americans accessing the care they need, and is working relentlessly to improve the resilience of the healthcare sector to cyberattacks.[1] **We must continue to move away from a mentality that punishes those that have been victimized by malicious actors and criminals.**

CISA states, that: "While not part of the proposed rule, CIRCIA recognizes the value of these activities [the proposed collection of information and requirement of covered entities to report covered cyber incidents and ransom payments to CISA within the timeframes] and imposes upon CISA a number of requirements related to the analysis and sharing of information received through CIRCIA Reports to ensure their value is reasonably maximized." CISA further outlines these obligations[58] as required by CIRCIA.

CHIME and AEHIS members are extremely disappointed that in this proposal, CISA simply listed individual parts of the CIRCIA statute, and did not provide specific details on how they plan to fulfill these obligations – especially the requirement[59] to make information received in CIRCIA Reports available to appropriate Sector Risk Management Agencies (SRMAs) and other appropriate Federal agencies. All of the outcomes and benefits that CISA describes rely on timely, adequate, and bi-directional information distribution. CISA should have provided details in this proposal on how they plan to partner with SRMAs and

[57] Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double. (n.d.). In *Office of the Director of National Intelligence*. https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf
[58] 6 U.S.C. 681a(a)(1); 6 U.S.C. 681a(a)(2); 6 U.S.C. 681a(a)(3)(B); 6 U.S.C. 681a(a)(6); 6 U.S.C. 681a(a)(8); 6 U.S.C. 681a(a)(9); and 6 U.S.C. 681a(a)(10)
[59] 6 U.S.C. 681a(a)(10)

sector-specific ISACs to determine a plan by which the information will be distributed back to the sectors.

For example, under 6 U.S.C. 681a(a)(10), CISA is required to "as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 681c of this title, or information received pursuant to a request for information or subpoena under section 681d of this title, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies." **It is difficult for us to provide meaningful comment without knowing how CISA plans to disseminate relevant information to the ISACs and SRMAs – which for the HPH Sector, are the Health-ISAC and the Administration for Strategic Preparedness and Response (ASPR), respectively.**

In this proposal, CISA asserts that the information reported to them "will enable CISA to carry out its core statutory responsibilities related to identifying and sharing information on cyber incident trends, TTPs, vulnerability exploitations, campaigns, and countermeasures that may be useful in preventing others from falling victim to similar incidents and preventing similar vulnerability classes in the future." **If covered entities are required to submit a wide swath of information – under extremely tight deadlines – our members would expect that CISA would, in turn, be able to disseminate that information across the HPH Sector, or to those potentially at risk, in a similar or shorter timeframe.**

Simply having an "understanding of the threat and the vulnerabilities being exploited," without "the timely sharing of that information with owners and operators of internet-connected information systems so that they can take steps to better secure themselves from potential cyber incidents" – is woefully insufficient to execute the primary purpose of CIRCIA, which is to help preserve national security, economic security, and public health and safety.

CISA asserts, that: "By requiring CISA to perform these analytical activities and share information and analytical the findings with Federal and non-Federal stakeholders – an obligation CISA intends to fulfill through a variety of information sharing mechanisms, including through the development, maintenance, and issuance of publicly available alerts, advisories, a known exploited vulnerabilities catalog, and other products that can be leveraged by both covered entities and non-covered entities – CIRCIA will indirectly enhance the nation's overall level of cybersecurity and resiliency, resulting in direct, tangible benefits to the nation."

CISA already utilizes the "variety of information sharing mechanisms" listed in this proposal. This leaves CHIME and AEHIS members concerned that, as proposed, the lack of details on new information sharing mechanisms and the obligations outlined and required under CIRCIA – that the nation's, and our sector's, level of cybersecurity and resiliency will not be enhanced. F**urther, we are concerned that this proposal's lack of crucial details on information sharing back to the critical infrastructure sectors may mean that CISA will be unable to fulfill Congress's intent of CIRCIA. Direct, tangible benefits to the nation – across all of the sectors – absolutely relies on all of CIRCIA, not just parts of it.**

CISA requests comment on the potential impact of reporting requirements for preventing or mitigating cybersecurity incidents. **At minimum, we expected CISA to define and provide information, services and/or support that may be made available from the agency to the covered entity in response to the reports that they submit. A key component of CIRCIA is the requirement that CISA use the information it receives through mandated reports to**

issue intelligence products. Without specific proposals related to this requirement, CHIME and AEHIS are limited in our ability to comment on any potential impact for preventing or mitigating cybersecurity incidents.

Additionally, CISA requests comment specifically on what the consequences of a substantial cyber incident would be, the number of substantial cyber incidents expected in a given year, and how effective early notification of cyber incidents would be in mitigating expected consequences of an incident. As a recent example, during the early days and weeks after the Change Healthcare attack, our members found that it was extremely difficult to get access to needed information. It is our expectation that when – not if – the next seismic cyberattack strikes our sector, there will be a heightened level of transparency, coordination, and information sharing. **The ability to rapidly respond to cybersecurity incidents – and when possible, prevent them – while sharing information with our federal partners is essential to protect hospitals and HDOs.**

As previously mentioned, this proposal's lack of details on how, specifically, CISA plans to fulfill fundamental obligations required by CIRCIA, is disappointing, and does not allow for CHIME and AEHIS members to offer meaningful feedback or input. Of these obligations, we would have shared feedback on most – if not all – of the absent detailed information, especially how CISA plans to leverage information gathered about cyber incidents to provide appropriate entities with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures.[60] Additionally, we would have offered input on how CISA plans to aggregate and analyze reports to assess the effectiveness of security controls; identify TTPs adversaries use to overcome these controls; assess potential impact of cyber incidents on public health and safety; and enhance situational awareness of cyber threats across critical infrastructure sectors.[61]

However, we wish to share with you an example from just one of our members to express how essential the bi-directional, timely sharing of cyber threat information with the HPH Sector is. This member experienced a devastating cyberattack during the peak of the COVID-19 PHE. The time from threat actors initially accessing the environment to the deployment of ransomware across the entire virtual infrastructure, was less than one hour.

In less than one hour, a cyberattack devastated this member for not days, not weeks, but months. It took nearly a year before the paper records used during the aftermath of the attack were fully integrated back into their EHR. In the weeks that followed the attack, hospital staff were abruptly forced to use low-tech or no-tech methods for patient care – meaning not just whiteboards, pen and paper for medical records and notes – but for treating and monitoring patients. The oncology department – treating some of their most vulnerable, and hopeful patients – could not provide infusions or other treatments without first implementing temporary systems. In modern medicine, there are certain treatments for which there is no "offline mode." Meanwhile, any available staff shuttled between departments to provide clinicians with critical patient information, replace infected computers, and physically deliver medications and lab samples.

This example – one of many – highlights the importance of why disseminating bi-directional, timely information across and throughout the critical infrastructure sectors is so important. The lack of such details is disheartening and a significant oversight by CISA. American lives – and our member's patient's lives – may be saved by it.

[60] 6 U.S.C. 681a(a)(3)
[61] 6 U.S.C. 681a(a)(1)

Conclusion

In closing, CHIME and AEHIS appreciate the opportunity to comment on this proposed rule. As CISA garners and considers the input from the public in developing the final rule required by the CIRCIA, our members would appreciate continued opportunities to help inform the important work being done by CISA.

As previously mentioned – 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.

We look forward to continuing to be a trusted stakeholder and resource to you and continuing to deepen the long-standing relationship we have shared. Working together through the rulemaking process is just one way we can accomplish our shared goals and make meaningful changes in cybersecurity and healthcare – because at the end of the day, **cyber safety is patient safety.**

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