November 14, 2022

Jennie Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

Re: Docket ID: CISA–2022–0010
Submitted electronically via http://www.regulations.gov

Dear Director Easterly:

On behalf of the Workgroup for Electronic Data Interchange (WEDI), we write today in response to the publication of a Request for Information (RFI) in the September 12, 2022, edition of the *Federal Register* entitled "Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022" released by the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA). In this letter, we will provide feedback specifically on the issue of cyber incident reporting as well as offer our perspectives on a new approach to addressing ransomware reporting.

WEDI was formed in 1991 by then HHS Secretary Dr. Louis Sullivan to identify opportunities to improve the efficiency of health data exchange. WEDI was named in the HIPAA legislation as an advisor to the Secretary of HHS. Recognized and trusted as a formal advisor to the Secretary, WEDI is the leading authority on the use of health information technology (IT) to efficiently improve health information exchange, enhance care quality, and reduce costs. With a focus on advancing standards for electronic administrative transactions, and promoting data privacy and security, WEDI has been instrumental in aligning the industry to harmonize administrative and clinical data.

In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Public Law 117–103, Div. Y (2022) (to be codified at 6 U.S.C. 681–681g). Enactment of CIRCIA marks an important milestone in improving America's cybersecurity by, among other things, requiring CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransom payments to CISA. These reports will allow CISA, in conjunction with other federal partners, to rapidly deploy resources and render assistance to victims suffering

attacks, analyze incoming reporting across sectors to spot trends and understand how malicious cyber actors are perpetrating their attacks, and quickly share that information with network defenders to warn other potential victims.

Specific Comments on Cyber Incident Reporting

WEDI urges CISA to implement an incident reporting process that both meets the needs of a wide array of stakeholder types and is streamlined in such a way that does not overly burden those entities reporting a cyber incident. We make the following recommendations:

- Recognize the challenges smaller entities will face when reporting cyber incidents. Smaller providers, health plans and other types of health care entities may not have a robust information technology staff trained to recognize a security incident. As well, many smaller organizations outsource the information technology and security services. With this in mind, we recommend that the 48 hour "clock" start when the initial incident report is to be submitted start only when the reporting entity has definitively established that a cyber incident has taken place.

- Simplify the reporting process. Most importantly, the incident reporting process must be straightforward and easy for those reporting to complete. Ease of completion can be achieved by including comprehensive instructions that can be reviewed prior to starting the process, leveraging drop-down menus as opposed to free-form exposition as much as possible, and limiting the number of questions to the minimum required to achieve the purpose of the reporting.

- Create sample reports. CISA should consider developing sample cyber incident reports highlighting entities from different stakeholder categories, different sizes, and reporting different types of cyber incidents. These sample reports would offer guidance for the type of reporting that a covered entity would be expected to provide.

- Develop a web-based reporting process. We also recommend the reporting process be web-based. Options should include an online web portal and mobile application. Both should offer the ability of the user to save the information they have entered in case they need to stop at some point and come back to the form at a later time (for example, do conduct internal research or have discussions with colleagues). To support this process, we urge CISA to create a unique reference number to aid the reporting entity when they return to include updated information. The goal should be to reduce the reporting burden as much as possible and have the streamlined process serve as an incentive for those to report a cyber incident.

- Permit and encourage supplemental information to be reported. Further, the process should permit reporting entities to supply, at a later date, supplemental information or make revisions to information already reported. Cyber incidents are

rarely straightforward, and an entity's understanding of the incident can evolve as additional information comes to light. This is even more likely with the expedited timing requirements for the reporting entity. The process should actually encourage reporting entities to revise their earlier reports as they learn additional details regarding the incident. CIS should consider establishing timelines for reporting entities to submit additional information. However, these timelines should be long enough (for example, up to one year following the initial reporting) to accommodate complex situations where reporting entities face challenges in collecting supplemental information.

- Establish a secure reporting environment and protect the reported data. In terms of the data reported by impacted entities, it will be critical for CISA to ensure this information is kept secure. To be an effective tool, the process must collect potentially sensitive data pertaining to patient health information and internal security policies and procedures. CISA must deploy the appropriate measures to maintain a high level of security for both the data being reported via the web and all data collected. We recommend CISA include in the reporting instructions and on the web portal/mobile app the steps the agency is taking to ensure the security of the data is maintained and all associated privacy policies and procedures. We also recommend CISA specify how the reported data will be used, who will have access to the information, and how long the information will be retained.

- Third parties and cyber incident reporting. We recommend that the supporting regulations address issues related to third parties and cyber incident reporting. We expect that many covered entities will utilize the services of information technology and security third parties. However, we believe that while the covered entity should be required to include in its report that a third party was involved in the detection of the cyber incident, the mitigation of the incident, and/or the reporting of the incident, these third parties should be under no requirement to report a cyber incident independent of the covered entity.

- Consider grace periods. Cyber attacks are rarely straightforward and for many covered entities, they will have no experience dealing with this type of traumatic incident. We recommend establishing a grace period to the 72-hour deadline for reporting covered cyber incidents and for the 24-hour deadline for reporting ransom payments before imposing any enforcement action.

- Develop guidance. To assist covered entities, we encourage CISA to develop guidance on a wide array of cyber incident reporting issues. These should include how covered entities can recognize when a cyber incident has occurred, how to identify when the "clock" has started for the 72-hour deadline for reporting covered cyber incidents and for the 24-hour deadline for reporting ransom payments, what information the covered entity is required to collect, report and retain, and other topics.

- Avoid federal cyber incident reporting silos. There are numerous federal and state agencies that oversee issues related to ransomware and other forms of cyberattack. Many of these entities require cyber incident collection, with each having their own information collection processes and information retention requirements. It is imperative that the federal government ensure a single cyber incident reporting process is established and avoid circumstances where a covered entity is required by law to report the same incident to multiple agencies.

- Educate industry stakeholders. Reporting a cyber incident to a federal authority is a new process for covered entities. Covered entities, especially smaller organizations, will require training on the new reporting requirements and the reporting process itself. We recommend CISA work with its federal partners, including HHS, as well as private sector organizations such as WEDI to develop educational resources and outreach opportunities to better prepare the health care industry.

General Comments

Ransomware and malware pose a significant and growing threats to the health care industry. Malware refers to intrusive software developed by cybercriminals leveraged to steal health data and/or cause damage or destroy hardware and computer systems. Common malware intrusions include viruses, spyware, worms, Trojan viruses, and adware. Ransomware is unique from other forms of cyberattack, with a specific goal of denying the victim access to their own data, as opposed to removing or copying data, such as a medical record.

Smaller organizations and those located in rural areas of the country, simply are not equipped to ward off sophisticated cyberattacks and typically do not have sufficient internal technical expertise or necessary budgets to effectively meet these new cybersecurity challenges, despite being committed to securing their data. While reporting data breaches is required under the 2011 Omnibus regulation, the advent of more sophisticated cyberattacks in more recent times demand a revised approach to reporting, transparency, and enforcement.

Understanding how treacherous the current cyber environment is, the federal government must have access to accurate information regarding the scope and nature of these cyber-attacks if the health care industry is to have any reasonable chance of effectively combating cyberterrorism. Reports from entities experiencing a cyberattack, understanding exactly what tactics these criminals are using and what software they are deploying, providing actionable information to affected organizations on how to combat the attack, and amassing the intelligence necessary to prevent future cyberattacks is extremely vital. Without access to these data, developing and implementing a strategy to counter these criminal acts becomes close to impossible. Unfortunately, due to current policy, there is ample reason to believe HHS does not have a comprehensive picture of the scope of cyberattacks in health care due to its punitive and disciplinary approach to ransomware attacks.

Adopting a new approach to ransomware reporting

Ransomware presents a danger to all health care entities and the patients they serve. When addressing ransomware attacks, the current HIPAA Privacy and Security enforcement approach creates a culture of “blaming the victim.” We would argue that this approach should be changed to one focused on transparency and action. This revised approach will lead to improved cyber hygiene in the health care environment and a reduced threat to patient records and patient safety. When an organization is cyberattacked, not only is care coordination and data sharing impacted, but in some cases patient safety is threatened.

The federal government currently considers a ransomware attack a “data breach,” and thus entities attacked by ransomware are subject to the same process for both notification and enforcement as laid out in the breach notification provisions included in the 2013 HIPAA Omnibus regulation. We assert, however, that this equating of ransomware with a traditional breach of protected health information (PHI) is inappropriate. It is unreasonable and counter-productive for an entity to be penalized by the federal government for a ransomware attack that is beyond their control. We are concerned that the threat of punitive measures being imposed by the federal government following a ransomware attack could act as a deterrent against reporting the event.

It is also important to note that organizations experiencing a ransomware attack incur significant harm from the attack itself. The inability to access important data that an organization maintains can be catastrophic in terms of the lock out of sensitive patient information, disruption to regular operations (including the ability to treat patients), financial losses related to lost claims data, the expense incurred to restore systems and files, and the potential long-term harm to the reputation of the organization.

Ransomware is not typically a “use or disclosure of PHI” but rather extortion to unlock or regain access to data critical to the organization. This new, insidious form of attack on our nation’s health care infrastructure demands a new approach to information gathering and enforcement action. Therefore, we urge the federal government to consider adopting a ransomware policy that encourages entities to report cyberattacks and collaborate with the federal government in an investigation to mitigate the damage and ensure the safety of its patients.

Ransomware will remain a big part of the cybercriminal's portfolio in the next few years. The ability for an attack to shut down operations at a medical facility has life-or-death consequences in certain situations, which can motivate victims to pay the ransom. Cybercriminals know this, which explains the spike in healthcare-oriented ransomware incidents. A recent joint advisory by the Cybersecurity and Infrastructure Security Agency, HHS and the FBI says there is "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."

Ransomware presents a danger to all health care covered entities and the patients they serve and we urge the federal government to modify the current enforcement approach. We recommend moving away from a culture of “blaming the victim” to one focused on transparency and action. This revised approach will lead to improved cyber hygiene in the

health care environment and a reduced threat to patient records and patient safety. When an organization is cyberattacked, not only is care coordination and data sharing impacted, but in some cases overall patient care cannot occur. Understanding how treacherous the current cyber environment is, the federal government must have access to accurate information regarding the scope and nature of these attacks if the industry is to have any reasonable chance of effectively combating cyberterrorism. Real-time reports from CEs experiencing a cyberattack, understanding exactly what tactics these criminals are using and what software they are deploying, providing actionable information to affected organizations on how to combat the attack, and amassing the intelligence necessary to prevent future cyberattacks is extremely vital. Without access to these data, developing and implementing a strategy to counter these criminal acts becomes impossible. Unfortunately, due to current policy, there is reason to believe the federal government may not have a comprehensive picture of the scope of cyberattacks in health care due to its punitive and disciplinary approach to ransomware attacks.

Typically, a ransomware attack will encrypt an organization's data with a key known only to the hacker who inserted the malware. The hacker then demands a ransom be paid to release the data through use of a decryption key. In many cases, the perpetrator will instruct the victim to pay a ransom via an untraceable cryptocurrency, such as Bitcoin. In some cases, the health care sector has seen these criminals deploy ransomware with the ultimate goal of damaging or destroying patient data. Ransomware is therefore distinct from other breach-type events where PHI has been improperly disclosed to unauthorized individuals. Smaller organizations and those located in rural areas of the country, simply are not equipped to ward off sophisticated cyberattacks and typically do not have sufficient internal technical expertise or necessary budgets to effectively meet these new cybersecurity challenges, despite being committed to securing their data. While reporting data breaches is required under the 2011 Omnibus regulation, the advent of more sophisticated cyberattacks in more recent times demand a revised approach to reporting, transparency, and enforcement.

A ransomware attack is currently considered a data breach, and thus covered entities attacked by ransomware are subject to the same process for both notification and enforcement as laid out in the Breach Notification Rules contained in the 2013 HIPAA Omnibus regulation. We assert, however, that this equating of ransomware with a traditional breach of PHI is inappropriate and should be changed. Although the broad definition of a breach as an "impermissible use or disclosure of protected health information" may apply to certain ransomware attacks, we believe there are inherent differences between the two threats to PHI. Ransomware is unique from other forms of cyberattack, with a specific goal of denying the victim access to their own data, as opposed to removing or copying data, such as a medical record.

It is unreasonable and counter-productive for covered entities to be penalized by the federal government for a ransomware attack that is beyond their control. We are concerned that the threat of punitive measures being imposed by the federal government following a ransomware attack could act as a deterrent against reporting the event. It is also important to note that organizations experiencing a ransomware attack incur significant harm from the attack itself. The inability to access important data that an organization maintains can be catastrophic in terms of the lock out of sensitive patient information, disruption to regular operations (including the ability to treat patients),

financial losses related to lost claims data, the expense incurred to restore systems and files, and the potential long-term harm to the reputation of the organization. Ransomware is not typically a use or disclosure of PHI but rather extortion to unlock or regain access to data critical to the business. This new, insidious form of attack on our nation's health care delivery settings demands a new approach to information gathering and enforcement action. Therefore, we urge the federal government to adopt a ransomware policy that encourages covered entities to report cyberattacks and collaborate with the federal government in an investigation to mitigate the damage and ensure the safety of its patients.

We strongly recommend the federal government institute a policy to establish that ransomware is not considered a data breach when the covered entity has deployed a recognized security program and when no PHI has been accessed. Should no breach of the data occur that results in data being accessed by unauthorized entities and the covered entity be found to have a made good faith effort to deploy a recognized security program and instituted security policies and procedures, the covered entity should not be deemed to have experienced a data breach.

Conclusion

We appreciate the opportunity to share with CISA our perspectives on cyber incident reporting and ransomware issues. CISA has the important task of developing a cyber incident reporting process that meets the needs of a wide variety of covered entities. To decrease burden for those required to report, we urge CISA to continue to work with other federal agencies to create a single federal cyber incident reporting procedure. We also recommend partnering with the appropriate public and private sector organizations to educate covered entities on how best to avoid cyber incidents and how to report on it should one occur. Please contact Charles Stellar, WEDI President & CEO, at cstellar@WEDI.org to discuss these comments or explore opportunities to work together to educate impacted stakeholders.

Sincerely,
/s/
Nancy Spector
Chair, WEDI

cc: WEDI Board of Directors