April 25, 2022

James K. Olthoff. Ph.D.
Under Secretary of Commerce for Standards and Technology and
Director, National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Submitted electronically via regulations.gov

Dear Dr. Olthoff:

On behalf of the Workgroup for Electronic Data Interchange (WEDI), we write today in response to the publication in the February 22, 2022, edition of the *Federal Register* entitled "RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management" (87 FR 9579). WEDI appreciates the National Institute of Standards and Technology (NIST) requesting public comment on these important resources.

WEDI was formed in 1991 by then Department of Health and Human Services (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.

General comments

We first wanted to commend the NIST Applied Cybersecurity Division for its excellent work on the current "Framework for Improving Critical Infrastructure Cybersecurity" (CF) and for the many other resources the Division has developed to assist the industry meet cybersecurity challenges. With this Request for Information (RFI), NIST is seeking information to assist in evaluating and improving its cybersecurity resources, including the CF and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains.

We have divided our comments into three categories. The first focuses on the NIST CF and opportunities to add, delete, or modify the contents of the Framework. In the second category we will raise issues regarding the application of the CF-how the Framework be more effectively deployed to assist the industry meet the growing cybersecurity challenge. The final category of comments are recommendations in the area of supply chain-related cybersecurity.

In our response, we will focus how the CF and supply chain resources can be modified and mobilized to better address the following critical issues that we believe the health care industry will face in the coming years: (i) Cybersecurity intrusions (malware and ransomware); (ii) the security threat from third-party applications (apps); (iii); security of portable and implantable devices; (iv) lack of staff cybersecurity awareness and training and (v) lack of access to model cybersecurity policies and procedures. We believe NIST, through wide deployment of an updated CF and other cybersecurity resources, can assist the industry meet these challenges. In addition, we urge NIST to:

- Avoid federal government cybersecurity silos. Many agencies within the federal government, including NIST, are actively working on health care-related cybersecurity issues. These include the Centers for Medicare & Medicaid Services, the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the Office for Civil Rights, the Office of the National Coordinator for Health Information Technology, and others. We urge coordination in the development of policy, resources, and education.

- Expand educational partnerships. We thank NIST for partnering with WEDI on a recent educational event. We recommend that NIST staff experts and agency resources be leveraged to further acquaint the industry of the NIST resources and educate them on action steps to improve cyber hygiene. In addition to continuing our successful partnership, we encourage NIST to reach out to organizations representing various stakeholders in the health care sector and partner on cyber education.

Modifying the Cybersecurity Framework

WEDI applauds NIST for developing the CF and for engaging with the private sector to continue augmenting this important resource. The CF is well established as an essential document leveraged by each sector comprising the critical infrastructure of the nation. For the health care sector, the CF represents the benchmark for those seeking to develop a comprehensive cybersecurity program. The following are our specific comments and recommendations on modifying the CF to make this already excellent resource stronger:

- Include an increased focus on ransomware. We commend NIST for publishing in February 2022 the Ransomware Risk Management: A Cybersecurity Framework Profile. This Ransomware Profile resource includes security objectives that support identifying, protecting against, detecting, responding to, and recovering from ransomware events. It contains valuable information and tips to assist organizations combat ransomware. Our recommendation is that NIST consider

modifying this resource in the following ways:

- Incorporate the ransomware issue directly into the CF. The immediate and persistent threat of ransomware attack is driving a lot of resource allocation on the part of health care entities and by incorporating the ransomware issue directly into the CF NIST will expand the reach and impact of this resource.

- Include specific case studies (potentially de-identified) of health care organizations that have experienced a ransomware attack. These case studies could involve organizations of different sizes and from different sectors of the health care industry.

- An updated resource could focus on contingency planning, execution, and recovery. When a health care entity is hit with a ransomware attack, there can be a devastating impact to operations. For example, if a cloud-based electronic health record vendor is attacked, their client base of physician practices, hospitals, and other care settings could experience a loss of functionality that affects care delivery.

  Expanding the CF to define contingency planning strategies based on the type of health care entity hit with the attack would also be beneficial. Most important will be inclusion of examples of how vendors, providers, and health plans have mitigated these attacks and deployed contingency plans to minimize impact on patient care.

- Address the security challenge of third-party apps. Many HIPAA Covered Entities (CEs), including health plans, physician practices and inpatient facilities have already built or have contracted with business associates to develop patient access Application Programming Interfaces (APIs) and applications (apps) and are actively promoting their use.

  Specifically, these apps deployed by providers and health plans are typically covered under HIPAA and therefore the individual's accessing data have assurances that their information is being kept private and secure. We are concerned, however, regarding the lack of robust privacy standards applicable to the large percentage of third-party app developers not directly associated with CEs and therefore not covered under HIPAA. We note as well that there currently is no federally recognized certification or accreditation for these apps.

  The potential exists for Protected Health Information (PHI) gained via the apps to be inappropriately disclosed to the detriment of patients and their families. While we strongly support patient access to their PHI via apps, we assert that a national security framework, perhaps developed by NIST, is required to ensure that health care data obtained by third-party apps is held to appropriate privacy and security standards.

- Address portable and implantable medical devices in the CF. The use of connected portable and implantable devices, including implantable cardiac stimulators, heart monitors, neurostimulators, hearing aids, and insulin pumps have grown rapidly in recent years. Just as any Bluetooth headset or phone, connected medical devices are vulnerable to cyberattack. The difference with medical devices is that a cyberattack could result in physical harm to the patient. When it comes to medical devices, privacy and security risks are tangible and need to be addressed. Most of these threats are linked directly to: (i) Bluetooth connectivity; (ii) Windows; (iii) Cloud; (iv) and Wireless keyboards.

  We believe the number of cybersecurity threats against medical devices is going to exponentially increase in the coming years as more and more health issues are address using connected medical devices. We recommend NIST address cybersecurity issues related to medical devices in the CF.

- Include the issue of insider threats in the CF. Insider-based threats fall into two broad categories-intentional and unintentional. While unsettling, some cybersecurity incidents are the result of specific and intentional acts on the part of a current or former employee. Employees with knowledge of network setup, vulnerabilities, and access codes pose an enormous threat to a health care organization. Employees with malicious intent could alter, destroy, or hold ransom critical and sensitive patient information. With so much attention and money surrounding cybersecurity in the health care industry, disgruntled current or former employees may decide to purposefully disclose patient information out of spite or for the potential of financial benefit.

  Data breaches caused by employee mistakes, such as a lost laptop, are also a common threat in health care organizations. The health care sector experiences more data breaches than any other industry. In 2021, health care breaches, from all causes, impacted an astounding 45 million individuals. The need for proper device management and monitoring, as well as the protection of sensitive information is equally as important to providing medical care for patients.

  Another threat to health care organizations through their employees are phishing attacks. A phishing attack is an attempt to trick users into revealing passwords or personal information. These cyber-attacks are a form of social engineering and are commonly transmitted via email. An employee may receive an email from a hacker posing as a platform used by the organization and say that their account password is no longer valid. If the employee is not properly trained on how to recognize these phishing emails, their 'click' to reset the password is all that a hacker needs to put an organization at risk.

  Each of these insider issues represent significant challenges for health care organizations. We recommend NIST address these in the next iteration of the CF.

- Develop a CF targeted at smaller organizations. Although mandated privacy and security requirements from HIPAA have been in place for many years, many smaller health care organizations and those located in rural areas of the country do

not have the resources to stay informed with and implement up-to-date security measures and protocols. This vulnerability provides an opportunity for cybercriminals to easily gain access to protected health information. A loss of patient social security numbers, contact information, prescriptions, test results, and financial information can be devastating to the patient and irreparably harm the impacted organization.

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

With this as the backdrop, we recommend NIST consider developing a CF-type resource aimed specifically at smaller organizations with limited technical expertise in cybersecurity. This resource could focus on detailing, in non-technical terms, the various threats facing smaller organizations, proactive steps that could be taken to mitigate risks, actions to take should the organization experience a cyberattack, and contingency plans to ensure patient care is not disrupted.

- Include case studies in the CF. We believe the CF would be even more valuable to health care and other industries by integrating case studies to illustrate key component of the Framework. These case studies could be either fictious or real-world with the name of the organization redacted. These practical applications of the CF would be most helpful, especially with organizations with limited technical expertise.

- Incorporate additional best practice guidance into the CF. With passage of H.R. 7898 in January 2020, the Health Information Technology for Economic and Clinical Health (HITECH) Act is revised to require HHS to consider efforts by CEs and business associates (BAs) to implement "recognized security practices" when assessing fines or penalties under the HIPAA Security Rule. The statute provides that if a CE or BA can demonstrate compliance for the previous twelve months with "recognized security practices," then that entity may benefit in the following scenarios: (i) mitigation of fines related to a HHS investigation resulting from a security incident; (ii) an early and/or favorable termination of an audit brought under section 13411 [of HITECH]; and (iii) mitigation of remedies agreed to in any agreement with respect to resolving potential violations of HIPAA Security Rule.

  Specifically, section 13412 of the Act states *"(1) RECOGNIZED SECURITY PRACTICES.—The term 'recognized security practices' means 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)."

Under this new law, HHS may reduce fines and penalties for certain violations for HIPAA-covered entities that have adopted cybersecurity best practices. These best practices and standards are those developed under the NIST Act and under 405(d) of the Cybersecurity Act of 2015. Considering the recent legislative requirement that HHS take into account a covered entity's deployment of "recognized security practices" before taking any enforcement action, we urge NIST to develop CF-based set of specific action steps that covered entities can leverage.

- Target a CF-based resource at consumers. The protections afforded by HIPAA privacy and security have been a fixture in our health care system for more than two decades. These privacy and security rules lay out a framework to ensure that PHI will be kept secure, and patients rely on HIPAA to ensure that the confidentiality of their information is maintained. Organizations that are CEs under the law have a responsibility to take necessary steps to maintain the trust of individuals. However, these same individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA CE or under a business associate agreement are not afforded HIPAA privacy and security protections.

  We continue to be concerned that patients will not have adequate information to be educated consumers regarding the potential dangers associated with, for example, exchanging PHI with third-party apps and may not fully comprehend that they are assuming the risk of the security practices implemented by their chosen app. Specifically, patients may not understand when their information is and is not protected by HIPAA.

  We urge NIST to consider developing a resource aimed specifically at consumers. This resource could outline specific dangers that consumers face when attempting to access, use, store, or exchange their health information in an electronic form. This guidance could follow the broader CF format (Identify, Protect, Detect, Respond, Recover) and apply it to consumer cybersecurity issues. We expect this Framework variation would be broadly disseminated by both patient and consumer groups.

- Stress a security-focused culture. The CF only very briefly addresses how an organization can effectively build a security-focused culture in its "Integrated Risk Management" section. We encourage NIST to augment this area and stress the importance of deploying appropriate security hygiene throughout an organization as an important step toward protecting data. Instituting cybersecurity staff training and ongoing education for every full and part-time employee. It is critically important for every health care entity to underscore that each team member is responsible for protecting patient data. NIST could develop an action plan that small, medium, and large-sized health care organizations could leverage as they created this security-focused culture.

Deploying the Cybersecurity Framework

The CF continues to be the benchmark for industry cybersecurity efforts. In addition to the CF, NIST has published a significant number of resources to assist critical areas of the nation's infrastructure improve cyber hygiene. It is imperative, however, that the CF and these other resources be effectively deployed to the sectors and organizations that most need them. We offer the following comments and recommendations to expand the reach of these critical NIST resources.

- Leverage the NIST partnership with the HSCC. The Health Sector Coordinating Council (HSCC) includes hundreds of private and public sector organizations. It represents a unique platform for development of and dissemination of cybersecurity guidance and resources. We encourage NIST to continue this collaboration and look for opportunities to leverage the NSCC to both disseminate existing NIST resources and leverage the expertise and experience of the wide and diverse HSCC membership to develop new resources.

- Private sector certification/accreditation. We note that the NIST CF is leveraged by many private sector cybersecurity accreditation and certification organizations such as the Electronic Healthcare Network Accreditation Commission (EHNAC) and HITRUST. While each accreditation and certification organization should be free to determine its own testing criteria, it will be important to operationalize the CF and make the framework an integral part of any private sector certification and accreditation programs. Combined, these organizations accredit and certify a significant number of health care entities so it will be important to build the next iteration of the CF into their programs as quickly as possible. We encourage NIST to work closely with these organizations to incorporate the revised CF into their respective programs.

- Work with WEDI, other industry groups to educate on the CF and supply chain cybersecurity. Utilizing conference sessions, webinars, and other educational vehicles, we recommend NIST continue to work with WEDI and other key health care stakeholders to educate our industry specifically on how the CF can be applied the health care stakeholders and the threat cyberattacks present to supply chains. Focusing on how to identify cyber threats, how to mitigate threats, how to develop effective contingency plans and how to successfully recover from an attack would be extremely beneficial to health care organizations.

Supply Chain Cybersecurity

We concur with NIST that addressing cybersecurity risk in supply chains requires ensuring the integrity, security, quality, and resilience of the supply chain and its products and services. We commend NIST for identifying the critical cybersecurity issues with supply chains: (i) Foundational practices; (ii) Enterprise-wide practices; (iii) Risk management processes; (iv) Risk; and (v) Critical systems. We offer the following comments and recommendations regarding supply chain cybersecurity:

- Recognize the various supply chain types in the health care sector. Like every critical infrastructure sector, health care has distinct supply chains. These include technology supply chains that support health plans (including cybersecurity technology, outsourced operations such as clearinghouse services, utilization management services, and claims payment services), and providers (including cloud-based electronic health record systems, clearinghouse services, and outsourced revenue cycle management services).

  As well, providers have supply chains that directly support patient care (including medications and vaccines, durable medical equipment, medical supplies, diagnostic equipment and servicing, personal protective equipment). Each of these supply chains are extremely vulnerable to cyberattack.

- Address the impact ransomware can have on health care supply chains. With the threat of ransomware growing in the health care sector, we recommend NIST address specifically how it can impact these supply chains. Again, we recommend leveraging the case study approach to provide real world examples of how a ransomware attack has impacted supply chains and how the organization reacted to and recovered from the attack.

- Address supply chain contingency planning. A cyberattack on a health care supply chain can have devastating impact on the care delivery process. It is imperative that health care organizations develop effective contingency plans to ensure that patient care is not negatively impacted in the event of a cyberattack. We recommend NIST work with the appropriate health care organizations to develop practical, action-oriented resources in this area.

Conclusion

We expect an increase in the number and types of threats targeting health care stakeholders as cyber criminals are deploying more sophisticated techniques every year. At the same time, while organizations have access to security resources that can reduce exposure and decrease the chance that patient data will be compromised, health care entities, especially smaller one, often operate on razor thin margins.

Allocating sufficient resources to address security issues if often a significant challenge. Recognizing this, the role of the federal government is to identify and make available to the industry the best possible protocols, policies, and procedures. We urge NIST to promote cyber hygiene tactics through every available communication channel, with an emphasis on smaller health care organizations.

We appreciate the opportunity to share our perspective regarding how to incorporate the new and expanded cybersecurity threats facing the health care industry into current NIST resources. WEDI believes the CF and other NIST resources represent some of the best cybersecurity resources available today. We hope our comments and recommendations will serve to improve the content of these resources and offer opportunities to expand NIST's outreach and impact on the health care sector. We must all work together to

ensure patient data is being securely maintained and exchanged throughout the health care ecosystem and provide patients increased confidence that their health information is being kept confidential.

Please contact Charles Stellar, WEDI President & CEO, at [redacted] to discuss these recommendations or explore future opportunities to work together to educate impacted stakeholders.

Sincerely,
/s/
Nancy Spector
Chair, WEDI

cc: WEDI Board of Directors