wedi™

Technology Today For A Healthy Tomorrow

March 7, 2025

The Honorable Robert F. Kennedy, Jr.
Secretary
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

RIN 0945–AA22
Submitted electronically via http://www.regulations.gov

Dear Secretary Kennedy:

On behalf of the Workgroup for Electronic Data Interchange (WEDI), we write today in response to the publication in the January 6, 2025, edition of the *Federal Register* entitled "HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information" released by the Department of Health and Human Services (HHS), Office for Civil Rights (OCR).

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 1996 HIPAA legislation as an advisor to the HHS Secretary. 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 for the improvement of health care.

The recent spike in cyberattacks reveal just how serious the vulnerabilities are throughout the U.S. health care system. The attacks also alerted industry leaders and policymakers to the urgent need for enhanced cybersecurity and improved business continuity planning to support redundancies and restoration when unplanned outages impact the delivery of health care services. In response to this NPRM, WEDI has identified important issues that should be addressed by HHS to mitigate the potential impact of a cyberattack on health care operations. We submit our comments on these regulatory proposals and offer additional recommendations for cybersecurity resources and building outreach programs to educate impacted stakeholders.

WEDI MPA Process

To identify comments for this NPRM and recommendations related to mitigating the impact of a cyberattack on health care data exchange, WEDI leveraged our Member Position Advisory (MPA) process which included workgroup discussions and a dedicated session on the NPRM. Our MPA event took place on February 11, 2025 and engaged almost 100 WEDI members through a virtual platform representing health plans, providers, clearinghouses, health IT vendors, standards development organizations, and others. The MPA event provided a unique venue to discuss proposed provisions included in the NPRM and additional dialogue centered on opportunities to reduce the threat of a cyberattack and mitigate the impact of a cyberattack on health care operations.

General Comments and Recommendations

- The Industry Recognizes the Growing Threat of Ransomware Attack.
  Health care organizations today are greater targets for cyber theft than organizations in other sectors for a few important reasons. The personal health data and research information facilities hold represent high value commodities to cyber criminals, including nation state actors. Decentralized information systems, where a vendor may use the services of one or more subcontractors, provide for a greater number of potential access points for incursion, putting patient care and privacy at risk. Regardless of their size, health care organizations make attractive cyberattack targets. First, they are financially lucrative targets because of the value of protected health information since attackers adjust ransom amounts to the perceived ability of the target to pay, attackers often will hold health information systems hostage until they have extracted maximum ransom payments, utilizing sophisticated tactics to transfer breach threats across criminal enterprises.

  Even if no money is paid, the extortion attempt by cyber criminals can still result in extended periods of downtime of the health information system with substantial (and very public) impacts to IT and patient services. The extensive media coverage of cyberattacks on health systems increases the pressure on victims to pay the ransom quickly before it becomes public. Additionally, many health organizations lack the resources to invest in modern, secure IT systems and strengthened cybersecurity defenses, often relying on outdated or legacy systems that are vulnerable to exploitation. Health organizations can also lack the capacity to respond to and mitigate cyberthreats, which increases the harm caused by cyberattacks as well as the probability of paying ransoms. Another serious consequence is the potential erosion of the patient's trust in the overall health care system.

  Recent cyberattacks, while unprecedented, are just the latest example of what has become unfortunately all too commonplace in the health care industry. No health care organization is immune to the threat of cyberattack and countering these threats will require a collaborative effort between the public and private sectors.

The following are recommendations we believe will assist the health care industry in preventing cyberattacks and mitigating the impact of a cyberattack on health care data exchange.

- Create the Office of National Cybersecurity Policy
  The federal government should create a new office called The Office of National Cybersecurity Policy (ONCP); an office led by a "Cyber Policy Czar." While we appreciate that there currently is an Office of the National Cyber Director (ONCD), this office is restricted to performing in an advisory capacity, with no authority to harmonize and coordinate actions taken by other federal agencies before during or after a cyberattack.

  We believe an ONCP could be modelled on the existing Office of National Drug Control Policy (ONDCP) and also be a component of the Executive Office of the President. ONDCP leads and coordinates the nation's drug policy and is responsible for the development and implementation of the National Drug Control Strategy and Budget. ONDCP coordinates across 19 federal agencies and oversees a $41 billion budget as part of a whole-of-government approach to addressing addiction and the overdose epidemic. ONDCP also provides hundreds of millions of dollars to help communities stay healthy and safe through the High Intensity Drug Trafficking Areas Program and the Drug-Free Communities Program.

  The recommended ONCP would not replace any existing agency or usurp any other agency's jurisdiction or function, but rather drive a centralized process of cyber incident reporting, coordinating harmonization efforts across federal agencies stakeholder education (with a focus on under resourced organizations), steer funding for stakeholder cyber preparedness, develop and deploy national contingency planning, and serve as the point agency for industry recovery following a major cyber incident.

- Implement a National Health Care Cyber "Fire Drill"
  HHS should designate a week as "National Health Care Cyber Fire Drill Week." This would be a designated period (i.e., a week) where HHS (or an ONCP) would lead the health care industry in promoting cyber awareness and action. Health care organizations would be encouraged not only to test internal systems and processes but also to work with their critical trading partners to identify and test systems, alternative data exchange pathways, and contingency plans.

  The Fire Drill should focus on: (i) improving overall cyber hygiene; (ii) internal testing; (iii) employee training; (iv) external testing; (v) contingency planning; (vi) disaster recovery planning; (vii) backup systems/disaster recovery testing; (viii) business continuity testing (trading partner outreach); (ix) awareness of available cybersecurity resources; and (x) other appropriate issues.

- Conduct Select Audits and Educate the Industry
  HHS, through OCR, should conduct proactive, comprehensive select audits of the health care sector. Past OCR audit programs have reviewed policies and

procedures adopted by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits should be continued as they present an opportunity to examine mechanisms for compliance, identify best practices, and discover risks and potential vulnerabilities. Specifically, OCR should be directed to conduct audits of those covered entities that experienced a cyberattack. Gaining first-hand knowledge of how the attack occurred, systems impacted, contingencies adopted, and post-attacks steps taken could be leveraged to assist other organizations. Through these select audits, OCR can identify best practices that will provide guidance targeted to address compliance challenges.

The aim of the new round of select audits would be to identify cyberattack vulnerabilities of HIPAA covered entities. Rather than conduct these select audits for enforcement purposes, we recommend they be conducted to assess the effectiveness of the current security controls and security gaps (and identify lessons learned) to update controls as appropriate to mitigate risk across the health care infrastructure.

De-identified results from these audits should be leveraged in an educational campaign to better prepare covered entities to address cyber threats. Educational campaigns should be targeted at specific stakeholder groups, sectors that are more frequently targeted by cyber criminals, and those that have limited resources. We encourage HHS to work with industry groups such as WEDI as well as stakeholder-specific professional associations to expand the reach of these important messages.

- Avoid Automatically Designating a Ransomware Attack as a Data Breach
  HHS 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 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.

  It is unreasonable and counter-productive for an entity to be penalized by the federal government for a ransomware attack, as well as the scramble to fulfill data breach reporting obligations in the midst of a cyber incident, 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 recommend a ransomware policy that encourages organizations to quickly report cyberattacks and collaborate with the federal government in an investigation to mitigate the damage caused by the cyberattack and ensure business continuity and the safeguarding of patients.

- Establish a Voluntary Audit Program
  OCR should be directed to establish a program that would permit covered entities to voluntarily undergo a security audit. This program could be modeled on the Department of Labor’s Occupational Safety and Health Administration’s (OSHA’s) Voluntary Protection Program (VPP) designed to promote effective worksite-based safety and health. In the VPP, management, labor, and OSHA establish cooperative relationships at workplaces that have implemented a comprehensive safety and health management system. The VPP sets performance-based criteria for a managed safety and health system, invites sites to apply, and then assesses applicants against these criteria. OSHA’s verification includes an application review and a rigorous onsite evaluation by a team of OSHA safety and health experts.

  OCR could emulate the approach adopted by OSHA by developing a program that would allow covered entities to have their security policies and procedures reviewed by OCR and any weaknesses detected. Those submitting their policies and procedures for voluntary review should not be subject to enforcement action should any deficiencies be identified during the audit. Rather, the organization should be given sufficient time to correct any issues. This program would be especially important for smaller organizations that do not have the resources required to engage a third-party accreditation/certification vendor.

- Encourage the Development and Support of Private Sector Accreditation/ Certification Programs
  For stakeholders or all types, sizes, and technical sophistication, having an independent, voluntary security accreditation would help ensure that the policies and procedures deployed by the covered entity were consistent with the regulatory requirements. Combining virtual (remote) testing of the requirements with self-attestation could substantially reduce the cost of the accreditation. Further, covered entities successfully completing an accreditation, should be considered meeting “recognized security practices” defined by the Health Information Technology for Economic and Clinical Health (HITECH) Act amendment, which allows health care entities to potentially lessen enforcement penalties if they implement security measures aligned with these recognized practices.

- Accredit the Accreditation Programs
  HHS should consider developing minimum standards for third-party accreditation/certification entities. As HHS highlights in this NPRM, we recognize that there is tremendous value in having independent entities review and

accredit/certify that an organization has met or exceeded its proprietary set of security requirements. However, we believe that a minimum set of security, privacy and cybersecurity standards should be mandated to ensure that an accredited or certified organization would be in the best position to avoid a cyberattack or mitigate the effects of a cyberattack.

We also recommend an analysis be undertaken to evaluate the current accreditation/certification bodies (both for profit and not-for-profit organizations) providing services in this space to understand how they are governed, what public and private sector standards are used as "baselines," and how are these standards measured.

Further, the minimum requirements for these accreditation/certification programs should include post attack actions including the implementation of best practices, policies, and procedures related to: (i) identifying and communicating with all trading partners that could potentially be impacted by the cyberattack; (ii) disaster recovery programs to mitigate the impact of a cyberattack on the organization and its trading partners; and (iii) contingency plans to ensure that the organization and its trading partners can continue data exchange following a cyberattack. Given our interconnected health care industry, every effort should be made to expand the coordination of testing programs.

- Avoid a "One Size Fits All" Approach
  One of the strengths of the 2003 Security Final Rule was the scalability of the requirements. It was recognized that not all covered entities will have the same technical knowledge, abilities, and resources and that there is a vast difference between, for example, a small provider office and a multi-state health system. In addition to accounting for the size and technical capabilities of an organization, HHS should also consider differences based on the role the organization plays in the health ecosystem. The final rule should recognize that not all covered entities will have the same resources and capabilities, and all regulatory requirements must be achieved at a reasonable cost. An independent assessment of NIST CSF maturity level[1], or achieving cybersecurity certification through programs such as HITRUST[2], CMMC[3], or ISO 27001[4], should be recognized by the Department to automatically reduce the frequency and scope of such review requirements on a sliding scale.

- Establish a Minimum Two-Year Implementation Glidepath
  The provisions included in the NPRM present a significant challenge for all covered entities. In many cases, they will require deploying new technologies, implementing new policies and procedures, and necessitate comprehensive training of staff and communication with business associates. With this in mind, we urge HHS to establish a minimum two-year implementation period from the effective date of the

[1] https://www.nist.gov/cyberframework
[2] https://hitrustalliance.net
[3] https://dodcio.defense.gov/CMMC/About/
[4] https://www.iso.org/standard/27001

final rule.

- Consider Staggering Implementation of the Regulatory Provisions
We contend that instituting a single "effective date" for all controls in a final rule would be a huge lift that would inevitably leave many covered entities out of compliance. We recommend HHS prioritize the various requirements and allow for a staggered schedule of effective dates based on high-priority baseline controls and provide additional time to implement more complex time-intensive controls.

- Allow a Continuation of Business Associate Agreements
Covered entities will require sufficient time to implement the various changes and allocate resources for compliance with the final rule, including modifying Business Agreements and other contractual arrangements with third parties. The transition conditions proposed are confusing and cumbersome. Consistent with our recommendation to develop a staggered timeline for the implementation of all required approved standards, we also recommend that once a final rule is effective, regulated entities should be allowed to continue operating under existing Business Associate Agreements until the Agreement renewal date, on or after the compliance date of the final rule. New Agreements would be executed to meet the updated Security Rule.

- Consider Deploying RECs to Assist Small Organizations
Regional Extension Centers (RECs), developed by HHS during the implementation of the CMS Electronic Health Record (EHR) Medicare Incentive (Meaningful Use) Program, represented a range of organizations that served local communities throughout the country. The focus was to provide on-the-ground technical assistance for individual and small provider practices, medical practices lacking resources to implement and maintain EHRs, and those who provide primary care services in public and critical access hospitals, community health centers, and other settings that mostly serve those who lack adequate coverage or medical care. RECs established themselves as trusted advisors for primary care and assisted providers in overcoming technical and workflow challenges to achieve success in the Meaningful Use Program.

  RECs could again be deployed to assist smaller, less resourced covered entities understand the cybersecurity regulatory requirements, identify and select appropriate security vendors, and deploy and document the required technology, policies, and procedures.

- Develop a Centralized, Comprehensive Website for Educational Materials and Guidance to Support Covered Entity Compliance
The Cybersecurity and Infrastructure Security Agency (CISA) has designated “Health Care and Public Health” as one of the 16 “critical infrastructure sectors.” With this designation, we believe it is in the nation’s best interest for OCR to develop a wide array of educational materials and guidance and to assist covered entities comply with regulatory requirements and house them in a central website. There are numerous resources available from multiple government agencies. This Center should house educational materials, guidance, use cases and examples, as

well as policy template examples for each of the required elements in the current Security Rule and any future regulatory requirements. As many covered entities lack the requisite security expertise or financial resources necessary to precure outside security consultants, establishing a Cybersecurity Resource Center would greatly assist the industry and decrease the chance of a cyberattack impacting the nation's health care system.

- Identify Opportunities to Reduce Industry Implementation Costs
  Our members believe the implementation costs identified in the NPRM, $9 billion the first year, $6 billion for years 2 through 5, underestimate the expected expenses related to meeting the proposed requirements. Even if they are accurate, these implementation costs are extremely high and would be imposed on an industry experiencing challenging operating margins. As the Department develops a final rule, we recommend exploring all opportunities to reduce costs for impacted organizations, including reducing the number of requirements, extending timeframes, and developing compliance resources to support the industry. The goal of this regulation is to improve the nation's ability to deliver and support health care. We urge HHS to avoid having as an unintended consequence of this regulation the crippling of business and clinical operations.

- Establish a Regular Cadence for the Updating of Security Standards
  We recommend HHS explore the feasibility of issuing new or updated security-focused standards to the industry on a regular yearly or bi-yearly basis. The advantage of this approach is that covered entities, business associates, and the vendors and consultants that assist them will know when to expect these updates and those required to implement them can adjust annual budgets accordingly. We note that HHS currently takes this approach in other areas of health care standards and technology updates, including yearly updates to the International Classification of Diseases, Tenth Revision and yearly updates to the EHR Incentive and Quality Reporting programs.

- Strike the Appropriate Balance Between Mandating Effective Cybersecurity Requirements and Not Imposing Undue Burden on Stakeholders
  We urge HHS to find the appropriate balance in the final rule between establishing a baseline set of requirements that will assist organizations protect themselves, their business partners, customers, and patients from the consequences of a cyberattack while not imposing an overly prescriptive and potentially financially devastating set of mandates.

Specific Comments on the NPRM

NPRM-Addressable Vs. Required (Pages 916, 917-918)

However, as we noted in 2003, the rule's flexibility of approach is primarily provided for in paragraph (b)(2) of 45 CFR 164.306 and in the standards themselves. The addressability feature merely provided an added level of flexibility in a way that the Department now believes is inadequate to ensure that regulated entities implement reasonable and appropriate security safeguards.

We believe that compliance with the implementation specifications currently designated as addressable is not—and should not be—optional, particularly in light of the shift to an interconnected and cloud-based environment and a significant increase in the number of breaches of unsecured PHI from both internal and external actors, regardless of the regulated entity's specific circumstances. Thus, we believe that it is necessary to strengthen the Security Rule to reflect the changes in the health care environment and the evolution of technology and to underscore that compliance with all of our proposals, if finalized, is required.

WEDI Comment

HHS introduced the concept of ''addressable'' implementation specifications in the 2003 Final Rule, where the rule distinguished "addressable" from ''required'' implementation specifications. We believe the goal of this 2003 provision was to provide covered entities with increased flexibility and recognition that not all organizations have the same technical capabilities. While none of the implementation specifications were optional, designating some of the implementation specifications as addressable provided each covered entity with the ability to determine whether certain implementation specifications were reasonable and appropriate safeguards for that entity, based on its risk analysis, risk mitigation strategy, previously implemented security measures, and the cost of implementation. We assert this approach would still be applicable, now more than two decades after publication of the 2003 Security Final rule.

NPRM-Technology Asset Inventory and Network Map (Page 937)

In place of the existing standard for security management process, we propose a standard at 45 CFR 164.308(a)(1)(i) that would require a regulated entity to conduct and maintain an accurate and thorough written technology asset inventory and a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI. The inventory forms the foundation for a fulsome and accurate risk analysis. A regulated entity must identify its information systems that create, receive, maintain, or transmit ePHI and all technology assets, as we propose to define them in 45 CFR 164.304, that may affect ePHI in such information systems in order to secure them.

In place of the existing standard for security management process, we propose a standard at 45 CFR 164.308(a)(1)(i) that would require a regulated entity to conduct and maintain an accurate and thorough written technology asset inventory and a network map of its electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI.

The standard would also require each regulated entity to determine the movement of ePHI through, into, and out of its information systems and to describe such movement in a network map. A regulated entity's network map would reflect where its technology assets are, for example, physically located at the regulated entity's worksite, or accessed through the cloud.

As another example, a covered entity might determine that ePHI is created, received, maintained, or transmitted by one or more offshore business associates (i.e., persons that are located outside of the U.S.) for such services as claims processing, call center staffing, and technical support, activities that inherently involve ePHI. The technology assets used by the business associate to create, receive, maintain, or transmit ePHI are not a part of the covered entity's electronic information system, but do affect the confidentiality, integrity, or availability of ePHI and so would be required to be included in the network map of the covered entity.

WEDI Response

We understand the value to a covered entity of establishing an inventory of all the organization's technology assets. An organization's asset inventory could include a detailed list of all IT assets like servers, computers, routers, switches, printers, software licenses, etc., with attributes such as serial number, purchase date, warranty status, and assigned user. The network mapping would be a visual representation of how these assets are connected within the network, showing relationships between devices through cables, wireless connections, and logical connections. The details needed for each component and keeping a current list of every software update/upgrade (like antivirus updates) will be a very large undertaking for covered entities. In particular, smaller organizations may lack the requisite expertise to develop these asset inventories and network maps. It is expected that many covered entities will incur significant costs to contract with outside consultants or firms to meet these requirements.

HHS proposes in this NPRM that regulated entities develop a full inventory of their technology assets and proposes a definition of "technology asset" that includes software, hardware, electronic media, storage systems, data, and all elements of what makes for a "relevant electronic information system." This also would reinforce what is subject to compliance includes both the systems that directly engage with ePHI and those that support the confidentiality, integrity, and availability of ePHI. The inventory of technology assets would establish the systems to be subject to all the proposed security requirements. In turn, this would define the scope for what would be subject to Security Risk Assessment requirements, full implementation of compliance measures, assessing the effectiveness of security measures, and the periodic evaluation of same to determine ongoing effectiveness. WEDI concurs that this would be a useful construct to set the expectation for what the scope of compliance efforts for HIPAA Security should be and compel a concreteness for regulated entities to have a firm grounding for that compliance effort.

We also agree with the need for covered entities to identify all assets that may affect the confidentiality, integrity, or availability of electronic protected health information (ePHI). The proposed rule would require regulated entities to conduct and maintain an accurate and thorough written technology asset inventory and network map. Once implemented, this network map would illustrate the movement of ePHI throughout the regulated entity's electronic information system(s) on an ongoing basis, but at least once every 12 months and in response to a change in the regulated entity's environment or operations that may affect ePHI.

While having an inventory and map is not an *explicit* requirement of the 2003 Security Rule, the NPRM notes it is a "fundamental component of conducting a risk analysis and many other existing requirements" under the current Security Rule. We agree that any technology assets a regulated entity uses to create, receive, maintain or transmit ePHI to a business associate would also need to be accounted for in the entity's technology asset inventory and network map.

As many covered entities may not have ever developed these asset inventories or network maps, we strongly recommend that HHS develop specific guidance and offer templates to assist organizations understand what technologies must be included in the inventory, how best to inventory the assets, and examples of network maps that could be relied upon by the organization.

NPRM-Software Patching (Page 943)
The proposed implementation specification for policies and procedures at proposed paragraph (a)(4)(ii)(A) would require a regulated entity to establish written policies and procedures for identifying, prioritizing, acquiring, installing, evaluating, and verifying the timely installation of patches, updates, and upgrades throughout its electronic information systems that create, receive, maintain, or transmit ePHI or that otherwise affect the confidentiality, integrity, or availability of ePHI. Under the proposed implementation specification for maintenance at proposed paragraph (a)(4)(ii)(B), a regulated entity would be required to review its patch management written policies and procedures at least once every 12 months and modify them as reasonable and appropriate based on that review.

WEDI Response
We believe that software patching can be an effective method of ensuring software is up-to-date and has the latest anti-virus capabilities. The challenge for many covered entities, especially smaller organizations, is that much of the software maintenance process is conducted by external vendors. We believe policies related to software patching can be done through business associates agreements and thus we believe incorporating software patching policies into business associate agreements should be a compliance option for covered entities, rather than require the covered entity themselves develop and implement patching policies. Further, we are aware that patching software could necessitate system downtime that could impact business operations or clinical care delivery. With that in mind, we urge HHS to permit covered entities to determine the value of software patching balanced against the other systems involved, risks at stake, and potential impact to business and clinical systems.

NPRM-Multi Factor Authentication (Pages 951, 998)
For the implementation specification on authentication management at proposed 45 CFR 164.308(a)(10)(ii)(C), we propose to require a regulated entity to establish and implement written policies and procedures for verifying the identities of users and technology assets

before accessing the regulated entity's relevant electronic information systems, including written policies and procedures for implementing MFA technical controls.
Cost Related to Regulated Entities Deploying Multi-Factor Authentication The Department estimates that, on average, regulated entities would have an information security analyst spend 1.5 hours deploying MFA, as specifically required under proposed 45 CFR 164.312(f)(2)(ii). This would be a one-time, first-year burden that includes an average of 30 minutes for a regulated entity to select an MFA solution that allows them to meet the requirements of the proposal without creating workflow disruptions or delays.

WEDI Response
We agree that Multi-Factor Authentication (MFA), when appropriately deployed, can be a critical step in defending against cyberattacks. While MFA is highly desirable and is recognized as an industry standard, the proposed rule appears to expand MFA to all internal and external systems. This is overly broad, and we therefore recommend MFA requirements apply when accessing internal networks with ePHI data from external networks, rather than applying universally. Once a user has passed from the external environment into the entity's internal environment through MFA as a mandated access control procedure, they should not be required to go through MFA again to access internal systems with ePHI.

In addition, we believe there are other areas where HHS should provide additional clarity regarding its compliance requirements. The first area involves whether MFA would apply to all clinical workflow situations. MFA could be counterproductive in a significant number of clinical areas. Clinician access to ePHI in, for example, an operating theatre or diagnostic testing suite, could require immediate access to ePHI and MFA could serve as a hindrance to the clinician gaining access to that information. Similarly, requiring MFA for a clinician already signed-on the system to authorize a clinical document or clinical order is not an efficient use of time. While MFA-based user authentication at the initial time of sign-on to access a system may be appropriate, once the clinician has initially signed-on, requiring MFA throughout the clinical workflow may serve to unnecessarily reduce workflow efficiency.

The second area we believe requires clarification is the application of MFA to authenticate the identity of a "technology asset." We urge HHS to provide examples of when MFA would be required, and when it would not be required. Also, it would be helpful to the industry to have HHS develop a non-inclusive list of examples of such authentication use cases.

We have concern with the estimate of 1.5 hours to deploy MFA. We believe that, regardless of whether a covered entity deploys proximity readers, phone apps, or other MFA technology, the time it would take for a consultant to review the organization's current authentication protocols and determine what approach would be best for that organization will take considerably longer than 1.5 hours. Additional time, of course, would be needed to actually deploy the new technology. We would anticipate that it would also take days or even weeks, depending on the size of the organization, to review MFA options, install, and test any new MFA technology.

NPRM-Incident Response (Page 954)

Under proposed 45 CFR 164.308(a)(12)(ii)(A)(2) and (3), the regulated entity would be required to implement written procedures for testing and revising the security incident response plan(s) and then, using those written procedures, review and test its security incident response plans at least once every 12 months and document the results of such tests. The regulated entity would also be required to modify the plan(s) and procedures as reasonable and appropriate, based on the results of such tests and the regulated entity's circumstances.

WEDI Response

We believe that incident response policies are critical to an organization's overall cyber hygiene. We concur with HHS that covered entities should be required to conduct incident response testing at least every 12 months. Of course, organizations can choose to test more frequently, based on their threat assessment. We note, however, that for many smaller organizations, developing an effective incident response policy may be beyond their capabilities. We urge HHS to develop incident response educational resources and policy templates.

NPRM-Restoration of Critical Systems (Page 955)

We propose to clarify that a regulated entity would be required to establish (and implement as needed) written procedures to restore both its critical relevant electronic information systems and data within 72 hours of the loss, and to restore the loss of other relevant electronic information systems and data in accordance with its criticality analysis.

WEDI Response

We appreciate the desire on the part of the Department to expedite the ability of a covered entity to restore both its critical relevant electronic information systems and data. We agree that restoring these systems as quickly as possible should be an imperative for the covered entity. We note as well that regardless of the type of covered entity, whether the impacted organization is a health plan, provider, or clearinghouse, they would be highly motivated themselves to retore critical business and clinical systems as quickly as possible.

We concur with the Department that covered entities should develop written procedures to restore critically relevant electronic information systems and data. Requiring this step will be important to ensure that health care systems incur minimal disruptions following a cyberattack. However, we recommend the Department not impose an arbitrary and overly aggressive time requirement. We have concerns that the current proposal for 72-hour restoration time is excessively prescriptive. Depending on the type of breach or cyber incident, it is important to know that it could take a covered entity 72 hours or more to simply recognize the depth and breadth of the cyberattack or intrusion. This need for additional time is even more likely with larger organizations with complex networks and multiple physical locations.

In addition, we recommend permitting covered entities to establish restoration timelines based on system criticality of the system, the nature of the cyber incident, and the extent of the damage incurred or the potential of damage. We also recommend that HHS allow for greater risk stratification as well as recognition that incidents vary by type and may require different timeframes to bring up safely without introducing new threats. We do agree that contingency plans should be tested regularly, with the best practice being no less frequent than every 12 months.

NPRM-Audit Timing (Page 955)
The final standard we propose under 45 CFR 164.308(a) is a new standard for compliance audits at proposed 45 CFR 164.308(a)(14). For this proposed standard, the Department proposes to require regulated entities to perform and document an audit of their compliance with each standard and implementation specification of the Security Rule at least once every 12 months. While the Security Rule does not currently require regulated entities to conduct internal or third-party compliance audits, such activities are important components of a robust cybersecurity program. The Government Accountability Office has published guidance on conducting cybersecurity performance audits for Federal agencies. Audits are typically conducted independently from information security management, and the function generally reports to the governing body of the regulated entity. This independence can provide an objective view of the regulated entity's policies and practices. According to the Institute of Internal Auditors, an internal audit provides ''[i]ndependent and objective assurance and advice on all matters related to the achievement of objectives.' An internal audit may be conducted by a business associate of a covered entity or a subcontractor of a business associate. These activities provide regulated entities with confidence in the effectiveness of their risk management plan.

WEDI Response
While WEDI in general supports the need for a review of a covered entity's compliance with the Security Rule, we are concerned with the overly prescriptive auditing requirement. Adding a yearly auditing requirement, especially calling for the covered entity to contract with an independent third-party to conduct the audit, imposes a significant administrative burden on all organizations.

Throughout this NPRM, HHS includes numerous requirements for covered entities to review and document policies and procedures. Also, covered entities are required to conduct a risk analysis at least once every 12 months. Auditing duplicates many of the same actions already required under this NPRM and would require significant expenditure of human and financial resources. At a minimum, we urge that the auditing requirement be met every 24 months to reduce the cost for covered entities. While an independent audit may be optimum to conduct out an expert review of an organization's technical and non-technical compliance with the requirements of the rule, we also recommend HHS offer auditing options for covered entities, including an option for self-attestation.

NPRM-Business Associate Verification and Certification (Page 956)
To assist regulated entities in complying with the new standard, we propose to redesignate the implementation specifications at 45 CFR 164.308(b)(3) as 45 CFR 164.308(b)(2) and propose to add an implementation specification for written verification at proposed 45 CFR 164.308(b)(2)(ii) that would require the regulated entity to obtain written verification from the business associate that the business associate has deployed the required technical safeguards. The Department proposes to require that the regulated entity obtain this written verification documenting the business associate's deployment of the required technical safeguards at least once every 12 months. Additionally, we

propose that the verification include a written analysis of the business associate's relevant electronic information systems. The written analysis would be required to be performed by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI to verify the business associate's compliance with each standard and implementation specification in 45 CFR 164.312.6

The Department proposes to require that the regulated entity obtain this written verification documenting the business associate's deployment of the required technical safeguards at least once every 12 months. Additionally, we propose that the verification include a written analysis of the business associate's relevant electronic information systems. The written analysis would be required to be performed by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI to verify the business associate's compliance with each standard and implementation specification in 45 CFR 164.312.625

We also propose to require that the written verification be accompanied by a written certification by a person who has the authority to act on behalf of the business associate that the analysis has been performed and is accurate. The proposal would permit the parties to determine the appropriate person to perform the analysis and how that person is engaged or compensated. This person may be a member of the covered entity's or business associate's workforce or an external party.

WEDI Response

We recommend HHS remove the requirement that the covered entity obtain written verification from business associates. If it is not removed, we urge the Department to revise the requirement to put the onus (compliance responsibility) on the business associate to provide their written verification to the covered entity. This approach would significantly reduce the burden on the covered entity having to reach out to multiple business associates to meet this requirement. We would also recommend that permitting self-attestation would be deemed sufficient for this requirement.

We also contend that there is duplication between the written verification and the written certification. We recommend that one or the other be eliminated from the requirements. Also, we urge HHS to develop model communication language that could be used by covered entities and their business associates.

NPRM-Documentation Requirements (Page 965)

As noted above, the current provision at 45 CFR 164.312 does not reference the documentation requirements in 45 CFR 164.316. Therefore, for clarity, we propose to explicitly require in 45 CFR 164.312 that documentation of technical safeguards conforms to the requirements in 45 CFR 164.316. This proposed change would clarify that a regulated entity must document the policies and procedures required to comply with this rule and how entities considered the flexibility factors in 45 CFR 164.306(b). It would also clarify that a regulated entity must document each action, activity, and assessment required by the Security Rule. The Department considers the documentation requirements and other provisions of 45 CFR 164.316 to apply to all of the safeguards, *including the technical safeguards, and this proposal is intended to remove any potential uncertainty among regulated entities.*

WEDI Response
We recommend that the Department provide clear guidance regarding specific types of documentation that typically need to be retained to support OCR investigations (e.g., OCR Audit Protocol). Without this guidance, regulated entities may feel compelled to unnecessarily save excessive amounts of data (e.g., securely saving irrelevant audit log entries for 6 years), further increasing the cost of compliance. We reiterate our recommendation regarding standard maintenance (above), i.e. review cadence, full in-depth review, and testing to align with the organization's cyber security maturity level

NPRM-Encryption (Page 968)
The Department proposes to add one implementation specification for the proposed standard for encryption and decryption. Specifically, proposed 45 CFR 164.312(b)(2) would require regulated entities to encrypt all ePHI at rest and in transit, with limited exceptions. Thus, a regulated entity would be required to encrypt all ePHI it maintains, as well as all ePHI it transmits, unless an exception applies, and the following conditions are met: • Each exception applies only to the ePHI directly affected by the circumstances described in the specific exception.

WEDI Response
We understand that deploying encryption technology can be an effective method of protecting ePHI. We recommend, however, that HHS be more specific regarding what technologies the encryption requirements would apply to. Organizations are likely to have other security controls in place, in addition to encryption. Therefore, we recommend modifying the language of this requirement by eliminating the word "all" to allow encryption flexibility based on risk and data protection strategy. This change would permit organizations to determine which IT components to encrypt, based on risk. Security-mature organizations typically rely on multiple and different data protection controls and a defense-in-depth strategy (e.g., dynamic network segmentation, data de-identification, access control, application firewall, database activity monitoring, etc.) to complement encryption. While encryption serves to protect data, a malicious actor in a ransomware attack can overlay its own encryption layer on top of existing encryption, effectively locking the data and blocking it from use until the ransom is paid. Risk-based flexibility supports a multi-pronged and more robust approach.

Also, it is important to remember that deploying comprehensive encryption programs can present financial challenges for covered entities. Encryption can be expensive, especially for large amounts of data. We also note that covered entities that require multiple layers of encryption will incur higher costs.

NPRM-Network Segmentation (Pages 967, 998)
Accordingly, we believe that it is appropriate to require regulated entities to deploy technical controls to segment the networks to which their relevant electronic information systems are connected. What constitutes reasonable and appropriate network segmentation depends on the regulated entity's risk analysis and how it has implemented its network(s) and relevant electronic information systems.

The Department estimates that each regulated entity would spend an average of 4.5 hours to set up network segmentation in the first year of compliance with a final rule (with a low estimate of 4 hours and a high estimate of 5 hours) at the hourly wage of an information security analyst.

WEDI Response
We heard from our members that network segmentation can prove difficult to implement for many organizations. Additional guidance from HHS is needed if the network segmentation requirement is finalized. For example, how exactly is “segmentation” to be defined and what would HHS constitute as "successful" segmentation? We heard from members that for many organizations, a complete network segmentation process could easily be a “multiyear plan” that would require a rebuilding of the entire network architecture as well as retesting and resecuring all applications and technologies tethered to the network.

We are also concerned that the estimate included in the NPRM that each regulated entity would spend an average of 4.5 hours to set up network segmentation in the first year of compliance with a final rule (with a low estimate of 4 hours and a high estimate of 5 hours) is significantly lower than what covered entities anticipate spending on this network segmentation requirement.

NPRM-Penetration Testing (Page 978)
The proposed implementation specification for penetration testing at 45 CFR 164.312(h)(2)(iii) would require a regulated entity to conduct periodic testing of the regulated entity’s relevant electronic information systems for vulnerabilities, commonly referred to as penetration testing. Penetration tests identify vulnerabilities in the security features of an application, system, or network by mimicking real-world attacks and are an effective way to identify weaknesses that could be exploited by an attacker. The proposal would require such testing to be conducted by qualified person(s). We propose to describe a qualified person as a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of ePHI. We believe that within the cybersecurity industry, it is understood that a person who is qualified to conduct such penetration testing is an individual who has a combination of one or more qualifying credentials, skills, or experiences to perform ‘‘ethical hacking’’ or ‘‘offensive security’’ of information systems. The proposal would require a regulated entity to conduct such testing at least once every 12 months, or in accordance with the regulated entity’s risk analysis, whichever is more frequent.

WEDI Comment
While we agree that penetration testing can be an important component of an organization’s cybersecurity processes, we urge HHS to consider the potential cost of mandating that this be completed by covered entities every 12 months. We believe that many smaller health care organizations do not have full-time, qualified IT security specialists and thus would be required to outsource penetration testing. Even organizations with internal IT security staff may lack the specialized expertise or necessary tools (both hardware and software) to conduct a high-quality penetration test.

We support the Department's well-intentioned proposals for vulnerability management. However, rather prescribing in detail what must be done, by whom, and when, we recommend allowing covered entities the flexibility to conduct vulnerability testing and penetration testing (different tests with different purposes and methodologies) as part of a rational risk management program that takes a prioritized, risk based, and threat-intelligence-based approach.

The NPRM estimates that organizations will average just three hours for penetration testing. We believe this figure significantly underestimates the time organizations will require for all the tasks associated with penetration testing. These tasks include vendor selection, planning, execution, reporting, review, and remediation. Most of these steps are not considered in the cost analysis included in the NPRM. According to one security resource, penetration testing can cost anywhere from $4,000-$100,000, with the average cost being $10,000-$30,000. Factors impacting penetration testing costs include the size and complexity of the organization, the type of penetration testing deployed, and, most importantly, what remediation steps are necessary to address the issues uncovered by the testing. We urge the agency to consider all costs associated with penetration testing as it develops its final regulatory requirements.

NPRM-Group Health Plan Requirements (Page 984)

Similar to the discussion above, the Department proposes to add a new implementation specification for contingency plan activation at proposed 45 CFR 164.314(b)(2)(v) that would require plan documents to include a provision requiring a plan sponsor to report to the group health plan without unreasonable delay, but no later than 24 hours after activation of its contingency plan. As discussed above, the Department believes that a group health plan needs to be notified in a timely manner when a plan sponsor activates its contingency plan because of the potential implications on the ability of a group health plan to protect the confidentiality, integrity, and availability of ePHI in its relevant electronic information systems.

Accordingly, we believe that 24 hours would provide a plan sponsor sufficient time to do all of the following: determine that there is an emergency or other occurrence adversely affecting the plan sponsor's relevant electronic information systems; determine that it needs to activate its contingency plan; activate its contingency plan; identify any group health plans that need to be notified; and notify such group health plans. Similarly, as discussed above, we propose to permit the group health plan and plan sponsor to negotiate the form, content, or manner of the notice and include them in their plan documents if they so choose. The Department believes that requiring a plan sponsor to provide prompt notice to the group health plan when the plan sponsor activates its contingency plan would enable group health plans and plan sponsors to maintain individuals' confidence in their commitment to protecting the confidentiality, integrity, and availability of ePHI.

WEDI Response

In general, we agree that if/when a plan sponsor has access to ePHI, it must implement expected administrative, physical, and technical safeguards, along with other similar obligations, to protect the confidentiality, integrity, and availability of ePHI consistent with all CEs. However, we strongly disagree with requiring the plan document (i.e., via a legal agreement) between the CEs and the plan sponsor(s) to contain these obligatory clauses. Rather, we recommend the Department's final rule clarify that health plans and health insurers are simply communicating the cybersecurity requirements to protect ePHI confidentiality, integrity, and availability to the plan sponsor(s); they do not have liability for a plan sponsor's potential non-compliance with the HIPAA Security Rule.

We have concerns with the proposal to require group health plans to include in their plan documents requirements for their group health plan sponsors to: (i) comply with the administrative, physical, and technical safeguards of the Security Rule; (ii) ensure that any agent to whom they provide ePHI agrees to implement the administrative, physical, and technical safeguards of the Security Rule; and (iii) notify their group health plans upon activation of their contingency plans without unreasonable delay, but no later than 24 hours after activation.

We believe it is imperative to make explicitly clear who exactly is covered under this portion of the rule. We note that these regulatory requirements could impact organizations that have never been covered entities under HIPAA and therefore would not have had to comply with its regulatory provisions. We are also concerned with the proposal that group health plan sponsors notify their group health plans upon activation of their contingency plans "without unreasonable delay, but no later than 24 hours after activation." Requiring notification within one day sets an unreasonable expectation and we recommend group health plan sponsors be given discretion in this area and additional time to complete this communication. We also recommend that should the contingency plan deployed by the group health plan sponsor be effective and there is no disruption to services, notification to the group health plans should not be required.

NPRM-Estimated Costs (Page 993)
The Department estimates that the first-year costs attributable to this proposed rule total approximately $9 billion. These costs are associated with regulated entities and health plan sponsors engaging in the regulatory actions described above. For years two through five, estimated annual costs of approximately $6 billion are attributable to costs of recurring compliance activities.

WEDI Comment
WEDI has concerns with the estimated cost to the industry of implementing this regulation. If the estimates are accurate, the associated cost for stakeholders to meet the requirements of the rule would pose a significant burden on many covered entities and business associates. Entities such as regional health plans, rural hospitals, small physician and dental offices, and less resourced business associates, may not have the internal expertise or the financial ability required to meet the comprehensive requirements detailed in the NPRM. Of even greater concern is the potential that the cost estimate outlined in the NPRM significantly underestimates the actual cost for the industry to implement the regulation.

The Department identified ten categories of quantifiable costs arising from these proposals that would apply to all regulated entities: (1) conducting a Security Rule compliance audit; (2) obtaining written verification from their business associates or subcontractors that the business associates or subcontractors, respectively, have conducted the required verification of compliance with technical safeguards; (3) notifying other regulated entities when workforce members' access to ePHI is terminated; (4) completing network segmentation; (5) disabling ports and removing extraneous software; (6) deploying MFA; (7) deploying penetration testing; (8) updating policies and procedures; (9) updating workforce training programs; and (10) revising business associate agreements. Each of these categories potentially will require significant internal resources and/or contracting with outside vendors or consultants.

The concern expressed by many of our members is that the time and resources devoted to meeting the comprehensive requirements included in this regulation would come at the expense of direct patient treatment and critical business functions. They also expressed concern that the unintended consequence of these proposals could be that some smaller organizations may literally be put out of business.

NPRM-Workforce Training (Page 995)
The Department assumes that most regulated entities would be able to incorporate changes to their workforce training into existing cybersecurity awareness training programs and Security Rule training rather than conduct a separate training because the total time frame for compliance from date of publication of a final rule would be 240 days.

WEDI Response
WEDI generally agrees with HHS that regulated entities will incorporate changes to their workforce training based on the new requirements. We agree that comprehensive workforce training is the best practice for all covered entities and business associates. However, we have concern that the process of first understanding the provisions included in any final rule, developing supporting policies, and then training the organization's workforce on what potentially could be massive changes to security policies and procedures, all within 240 days, is unreasonable. We recommend covered entities be given 2 years to implement any final rule.

NPRM-Risk Analysis (Page 1012)
2) Standard: Risk analysis—(i) General. Conduct an accurate and comprehensive written assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted by the covered entity or business associate.

WEDI Response
As HHS notes in the NPRM, OCR investigations revealed that many covered entities had failed to complete an appropriate risk analysis. We agree that a risk analysis is the core action that covered entities need to take to ensure ePHI is protected. We support the NPRM's focus on covered entities conducting a thorough risk analysis, explaining the difference between a risk analysis and risk management, and how best practices are to utilize risk decision-making regarding the ePHI handled with each business decision. We also recognize the value of the technology asset inventory to the risk analysis process. Organizations seeking to understand where their risks are related to ePHI must first know where ePHI resides and how it is transmitted. We also believe that a comprehensive risk analysis must include all information, not just hardware and infrastructure, and not just electronic information.

We appreciate the development of various risk analysis resources by the federal government, including the Assistant Secretary for Technology Policy, office of the National Coordinator for Health IT's Security Risk Assessment Tool, the National Institute for Standards and Technology's (NIST's) Risk Management Framework and others. We also note that NIST Special Publication 800-66 can be used by covered entities to facilitate the completion of the risk analysis process. We recommend that federal risk analysis resources be updated to address any changes included in the final rule, that HHS work with impacted stakeholders to ensure that these resources meet the needs of a wide array of end users, that these resources be included in a centralized online location, and that HHS actively disseminate these resources to the industry.

NPRM-Termination Procedures (Page 1014)

(C) Modification and termination procedures. (1) Establish and implement written procedures, in accordance with paragraph (a)(9)(ii)(C)(2) of this section, to terminate a workforce member's access to electronic protected health information and relevant electronic information systems, and to facilities where electronic protected health information or relevant electronic information systems might be accessed. (2) A workforce member's access must be terminated as soon as possible but no later than one hour after the employment of, or other arrangement with, a workforce member ends.

(D) Notification. (1) Establish and implement written procedures, in accordance with paragraph (a)(9)(ii)(D)(2) of this section, to notify another covered entity or business associate of a change in or termination of access where the workforce member is or was authorized to access such electronic protected health information or relevant electronic information systems by the covered entity or business associate making the notification. (2) Notification must occur as soon as possible but no later than 24 hours after a change in or termination of a workforce member's authorization to access electronic protected health information or relevant electronic information systems maintained by such other covered entity or business associate.

WEDI Response

WEDI agrees with HHS that there are potential threats associated with terminated employees potentially having access to systems and ePHI. We also agree that organizations need written policies and procedures governing role-based access to systems containing ePHI, with timely access review to ensure those whose jobs have changed, have moved jobs, and/or no longer need ePHI access, have their access removed. However, we are concerned with the overly prescriptive requirement that the termination of a workforce member's access occur within one hour of the termination and the requirement that other entities be notified within 24 hours. We contend that requiring such a rapid turnaround of for all workforce terminations is overly burdensome for employers. We disagree with the proposed rule that regulated entities would have to terminate a workforce member's access to systems containing ePHI within 1 hour of employment or another arrangement (e.g., contract) ending. This requirement is overly stringent, too prescriptive, and potentially infeasible under technical implementation and processing. In the case of an involuntary termination, this short timeframe would add more strain on the system for unplanned staff dis-embarkment.

Industry standards generally dictate that users first log into an entity's IT environment (the so-called "front-door") through a centralized rights management service (e.g., Active Directory), then log into specific applications and systems based on their job roles and authorized access. When a staff member ends their work relationship with the entity, the priority is to deny enterprise access ("locking" the front door). This prevents their ability to access the entity's internal environment and prohibits access to ePHI systems. This step sufficiently safeguards ePHI, while internal processes then may terminate specific system access according to an operational schedule. This process occurs under the entity's access management policies and procedures, including periodic access review and eliminating inactive accounts. We recommend the Department remove the 1-hour time limit.

Similarly, the 24-hour requirement to notify other regulated entities and BAs of a member's termination is also unreasonable and unnecessary, as applicable BA agreement language establishes the notification process agreed upon between regulated entities and BAs according to their contracted services, business priorities, and risk positions. Therefore, we also recommend removing the 24-hour notification time limit for regulated entities and BAs.

If the one-hour and 24-hour requirements included in the final rule, we recommend the Department consider an alternative that would permit covered entities to determine when high-risk situations require a one-hour termination procedure and notification of impacted critical parties within 24 hours. For low-risk terminations, covered entities should be given a minimum of 48 hours, to complete the termination process and at least 72 hours to notify impacted critical parties.

NPRM-Written Verification Proposal (Page 1016)

Written verification. Obtain written verification from the business associate at least once every 12 months that the business associate has deployed the technical safeguards as required by § 164.312 through both of the following: (b)(2)(ii)(A) A written analysis of the business associate's relevant electronic information systems by a person with appropriate knowledge of and experience with generally accepted cybersecurity principles and methods for ensuring the confidentiality, integrity, and availability of electronic protected health information to verify compliance with each standard and implementation specification in § 164.312. (b)(2)(ii)(B) A written certification that the analysis has been performed and is accurate by a person who has the authority to act on behalf of the business associate.

WEDI Response

We recommend that HHS eliminate the requirement that covered entities obtain written verification from business associates. This provision adds significant administrative burden on covered entities without producing discernable value. Should it not be eliminated, we urge the Department to revise the requirement to put compliance responsibility on the business associate themselves to provide their written verification to the covered entity. This approach would reduce the burden on the covered entity having to reach out to multiple business associates to meet this requirement.

Conclusion

We applaud HHS for recognizing the need for the health care industry to address the growing threat associated with cyber incidents. We are experiencing an unprecedented number of attacks on the health care sector, attacks that can impact business continuity and even patient safety. We appreciate the Department's focus not just on preventing or mitigating cyberattacks but also identifying important actions for covered entities to take to recover from a cyberattack and minimize disruption to business and clinical operations.

WEDI recommends that any final rule acknowledge that security policies and procedures cannot be packaged as one-size-fits-all. It is important to recognize there is a vast difference in resources, expertise, and capabilities between health care organizations. Each organization will need to take their own journey toward better cyber hygiene, and we urge HHS to develop and disseminate the necessary resources to make that journey successful.

WEDI supports the appropriate updating of the HIPAA Security Rule and improving the health care sector's cyber hygiene. At the same time, we urge HHS to strike the appropriate balance between mandating effective cybersecurity requirements and the cost to implement these requirements. We strongly urge HHS to not impose the type of administrative and financial burdens on covered entities and their business associates that could impact their ability to conduct business and deliver care to patients.

We appreciate the opportunity to share our perspective regarding the proposals included in the NPRM, the current security threats facing the health care industry, and sharing our recommendations on the actions HHS and the private sector can take to mitigate those risks. Please contact Robert Tennant, WEDI Executive Director, at rtennant@wedi.org to discuss these comments or explore opportunities to work together to educate impacted stakeholders.

Sincerely,
/s/
Merri-Lee Stine
Chair, WEDI

cc: WEDI Board of Directors