Submitted via *http://www.regulations.gov*

March 6, 2025

Acting Director Anthony Archeval
U.S. Department of Health and Human Services
Office for Civil Rights, Attention: HIPAA Security Rule NPRM
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue SW
Washington, DC 20201

RE: HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information (HHS–HHS–0945– AA22)

Dear Acting Director Archeval:

The Healthcare Trust Institute appreciates the opportunity to submit comments on the HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information notice of proposed rulemaking (NPRM or proposed rule) issued by the Office for Civil Rights (HHS) of the Department of Health and Human Services (Department or HHS) and published in the Federal Register on January 6, 2025.[1]

The Healthcare Trust Institute (HTI) is a coalition of healthcare organizations committed to promoting and implementing effective privacy and security protections for health information that engender trust in the healthcare system and allow for the advancement of treatments, cures and improved healthcare quality for individuals and populations. HTI members, which include companies and organizations from across the U.S. healthcare economy, agree that a strong national privacy standard for health information is needed to protect sensitive data and spur medical innovation.

The Health Trust Institute and its member organizations place the highest priority on protecting the privacy and security of protected health information (PHI). Our members recognize that without data safety there can be no patient safety, and that every essential health care function ultimately relies on patient data A 2020-2021 Healthcare Cybersecurity Report predicted that the global healthcare cybersecurity market will grow by 15 percent year-over-year over the next five years, and reach $125 billion cumulatively over a five-year period from 2020 to 2025.[2] Based on the most recent American Hospital Association (AHA) survey, U.S. hospitals and

[1] See 90 Fed. Reg. at 898 (January 6, 2025).
[2] See https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/.

healthcare systems increased their spending on cybersecurity even more, by 62 percent between 2021 and 2023. This spending is not driven by the need to comply with any particular regulations, but rather, by the need and desire to strengthen cybersecurity defenses so as to protect patient safety and wellbeing by protecting their data against increasingly sophisticated cyberattacks, many by state actors aimed at the health care sector and critical infrastructure of the United States. Despite large expenditures the cybersecurity maturity level and risk ratings of the healthcare sector as a whole, and of hospitals in particular, have lagged other sectors of the economy materially[3].

We therefore welcome and strongly support an update to the HIPAA Security Rule, and view it as an opportunity for health care organizations, in collaboration with HHS and government generally, to improve cyber defenses in the health care sector. As such, we view the update to the HIPAA Security Rule in a wider context of strengthening cyber resilience across all entities that hold consumer health data. This will require, in addition to an update to the HIPAA Security Rule framework, legislation to set a national standard to protect all health data as well as an ongoing and active role by the federal government in helping maintain the cybersecurity of health entities.

This should include the following:

- ongoing financial funding to support the health care sector in building cyber defenses to withstand the unprecedented and growing threat level, particularly for smaller health care entities that are frequently the targets of cyber criminals seeking the weakest links, but that lack the resources to stand at the frontline of cybersecurity defense for the health care sector
- a federal insurance fund in the event of major cybersecurity attacks
- a focus on building the cybersecurity workforce to address the shortfall in experienced cybersecurity professionals
- a collaborative cyber hub or dome to help develop cybersecurity defenses at the national level
- bi-directional data sharing between health entities and the government to allow for quicker and more effective responses to cyber.

It is only through this broader approach that includes all three prongs, namely, appropriate regulation, government support to help build cybersecurity resources, and bi-directional data sharing, that together we can build a safer, more resilient health care system that will be able to deliver on the promise of better care and improved health outcomes for all Americans.

We stand ready to work with the Department and other relevant government agencies to achieve these goals. It is in this spirit that we offer the below comments.

I. General Comments

The proposed rule would make the most significant changes to the HIPAA Security Rule since its promulgation over two decades ago. To support these changes, HHS cites to a number of factors, including increased cybersecurity attacks, changes in technology, and a misunderstanding, and sometimes even a disregard of, the HIPAA Security Rule requirements.

We strongly support proposed changes that would eliminate misinterpretations and misunderstandings, or that add clarifications to help regulated entities apply the Security Rule

[3] https://pmc.ncbi.nlm.nih.gov/articles/PMC8449620/

requirements. We therefore applaud removal of language or terminology, such as “addressable” implementation specifications, that has been wrongly interpreted as giving regulated entities the option to implement the specification if they so choose. We also support clarification that “technical” safeguards cannot be implemented simply by establishing policies and procedures, and requires the deployment of technical controls. These and similar changes are common sense, but important, updates borne of HHS experience enforcing the Security Rule.

However, we are concerned that HHS has gone far beyond these types of changes and set unrealistic time frames in the proposed rule. While purporting to retain the foundational underpinnings of the current Security Rule, such as flexibility and scalability, the proposed rule would transform the current Security Rule from a technology-neutral and risk-based framework to an overly prescriptive, technology-specific one-size-fits-all set of security mandates, which have to be reviewed, tested, updated, and documented constantly.

The proposed security improvements would come at enormous costs and administrative burden to the health care sector. These costs are grossly underestimated in the proposed rule’s Regulatory Impact Analysis (RIA). All HIPAA covered entities and business associates, irrespective of their size, cybersecurity maturity level, risk level, operations, or other unique features would be required to comply with these mandates. This includes small and rural providers, despite the HIPAA statute’s requirement that the Department take into account the ”needs and capabilities of small health care providers and rural health care providers” in adopting security standards. Many of these small and rural providers lack the resources to implement the many new costly and prescriptive requirements and will simply be overwhelmed by them. We are concerned that this will lead to consolidation in the industry, as smaller or less resourced health entities close, merge or sell their practices to manage the compliance burden.

We are particularly concerned by the breadth, specificity, and unworkable time frames of many of the requirements, as well as the multiple, redundant verification mechanisms, from annual compliance reviews to annual or more frequent maintenance reviews and testing to annual business associate technical control verifications. While we appreciate the intent of these measures, HHS does not appear to have considered their practical impact, utility, or cost, especially when considered cumulatively and for every regulated entity. We strongly encourage the Department to instead build upon the current risk-based flexible approach allowing regulated entities, through their risk analysis and risk management plans, to prioritize their security risks and determine how to deploy their cybersecurity resources most effectively within the parameters of the Security Rule’s standard.

We also ask that the Department consider building on its own ‘‘Cybersecurity Performance Goals,’’ (CPGs), which were developed in collaboration with the health care sector, in the updated Security Rule, , While the Department mentions the CPGs in the preamble, it does not incorporate them in, or use them as a framework for, the proposed rule. The Department’s CPGs take a much more considered, flexible, and scalable approach, with minimum and enhanced measures. This approach would allow regulated entities of all sizes and maturity levels to build up their cybersecurity resilience in a measured way based upon their own circumstances, resources, maturity, and risk level.

Finally, we note that in January 2021, Congress passed P.L. 116-321 amended the HITECH Act to require the Department to consider certain recognized security practices of regulated entities when making determinations relating to certain Security Rule compliance and enforcement

activities ("HITECH Amendment").[4] While this amendment is mentioned in the preamble to the proposed rule, the Department proposes no regulatory language to codify it in regulation or explain how the Department is implementing or interpreting its requirements. The Department has also issued no written guidance on its implementation, with the result that regulated entities have little to no insight into how it is being applied. This defeats the purpose of the HITECH Amendment, which was intended to encourage regulated entities to implement recognized security practices. We strongly encourage the Department to include regulatory language to implement the HITECH Amendment in a manner that allows regulated entities to understand what they need to do to have it apply, and how the Department will apply it.

In light of the above concerns, we urge HHS to modify the proposed rule to maintain a scalable, risk-based approach exemplified by the current Security Rule and to build into the regulatory text the HITECH Amendment's incentives for regulated entities to implement recognized security measures. Absent major changes that will be needed to address these concerns, HHS should consider starting afresh with its own CPGs as the basis for a more workable update to the HIPAA Security Rule.

If the Department proceeds with finalizing the proposed rule, we provide specific comments below to assist in achieving the balance needed to strengthen cybersecurity in healthcare.

II. Specific Comments

A. Applicability

The Department proposes to apply the standard compliance date of 180 days after the effective date of a final rule, stating that it does not believe that the proposed rule would pose unique implementation challenges that would justify an extended compliance period beyond the 180 days. It also states that while it recognizes that it is proposing to substantially revise the regulatory text, it believes that most of the existing Security Rule's obligations for regulated entities would not be substantially changed by the proposed modifications because the proposed changes merely codify and provide greater detail on existing requirements.

We appreciate the Department's sense of urgency in light of ongoing cybersecurity attacks on the health sector and their increasing sophistication. As the Department makes clear, nothing prevents regulated entities from increasing their cybersecurity defenses at any time to the extent they are in a position to do so, and they may also comply with some or all of the additional requirements in the proposed rule before the proposed compliance date. We are concerned, however, that many regulated entities would not be ready or able to comply with all the required changes by the proposed compliance date. To implement the proposed changes, updating contractual agreements alone is likely to take more than one year for many covered entities. HHS either overlooks or greatly underestimates all the activities, time, and effort that would be required to meet the proposed compliance timeframe, even assuming there are not financial, legal, and resource constraints.

HHS gives encryption of ePHI in transmission and at rest as an example of a new requirement that it believes will not require significant cost or effort to implement on the basis that "encryption is built into most software today, and where it is not, there are affordable and easily implemented solutions that can encrypt sensitive information." This is a misconception. As discussed in greater detail below, once encryption applied beyond the storage layer, it becomes complex and costly to implement, and may have a significant negative impact on performance,

[4] See Public Law 116–321, 134 Stat. 5072, adding sec. 13412 (Jan. 5, 2021) (codified at 42 U.S.C. 17941).

which must also be addressed. The Department makes no mention of any of these issues. Other new obligations include the requirement to create a technology asset inventory and network map, the latter of which would incorporate the relevant technology assets of most, if not all, business associates (or in the case of business associates, subcontractors). Many covered entities and business associates have a large number of business associates/subcontractors, oftentimes into the hundreds or even thousands for larger regulated entities. These and many other new requirements, including patch management, network segmentation, new back-up requirements and workforce security changes, would need to be implemented at the same time as regulated entities develop new security awareness training and retrain their entire workforce and revise and implement all their security policies and procedures. Updating and implementing policies and procedures alone is a major endeavor.

A rushed implementation in order to meet the compliance deadline would defeat the purpose of the proposed rule. Yet regulated entities would have no choice but to consider the quickest and easiest approach that appears to check off the compliance boxes. We urge the Department to reconsider the proposed compliance time frame and to instead consider a phased-in approach that could be based on the Department's own CPGs. Such an approach would require compliance with only the essential safeguards first within 12 to 24 months of the effective date of the final rule and then gradual implementation of the enhanced safeguards after that, as appropriate.

Recommendations:

- **HHS should consider a phased-in approach, requiring compliance with essential safeguards within 12 to 24 months after the effective date of the final rule, and then a gradual implementation of enhanced safeguards after that.**

B. Definitions

The Department has provided certain new definitions and modified definitions with the goal of clarifying the requirements and scope of the security standards. We appreciate the additional clarity, but are concerned that the breadth and ambiguity of many of the revised and new definitions will create practical and operational challenges and new uncertainties, as well as greatly increase costs in certain cases. Below are our comments on a few of the new and modified definitions to illustrate these concerns, but these concerns extend beyond these few definitions.

1. Relevant Electronic Information System. HHS proposes to define the term "relevant electronic information system" to mean an electronic information system that creates, receives, maintains, or transmits ePHI "or that otherwise affects the confidentiality, integrity, or availability of ePHI." HHS states that this definition would clarify the scope of regulated entities' compliance obligations and make clear that the Rule's requirements do not only apply to electronic information systems that create, receive, maintain, or transmit ePHI.

The addition of "otherwise affects the confidentiality, integrity, or availability of ePHI" significantly expands the scope of the Security Rule while at the same time creating uncertainty as to the extent of that scope. The Department's examples of systems that "otherwise affect" ePHI only add to the uncertainty since they encompass any system that connects to a server that contains ePHI or even a system that contains information that "relates to" a system that contains PHI. Taken together with the Department's interpretation of "under the same direct management control," a regulated entity could potentially be responsible for ensuring compliance with the HIPAA Security Rule by systems of other regulated entities or non-HIPAA components of a legal entity or even non-HIPAA vendors with which the regulated entity contracts for systems

that do not access ePHI in an endless and ever-widening daisy chain of connected and related systems. Not only would this quickly become unmanageable, but it would force regulated entities to treat distantly and indirectly connected systems as warranting the same level of security as those that actually access ePHI, misdirecting resource from areas of highest priority and greatest risk.

Given the breadth and uncertainty of this definition, its pervasive use in the proposed rule and its lack of alignment with existing standards, we urge the Department to collaborate with industry experts and standards development organizations to help establish clear, workable definitions and boundaries for systems involved in processing ePHI.

2. Security Incident. HHS proposes to modify the definition of "security incident" to include attempted as well as successful unauthorized interference with system operations in an information system. We recommend that HHS eliminate unsuccessful attempts, whether to access ePHI or interfere in system operations, since this vastly increases the volume of security incidents that must be reported with no practical benefit. Covered entities neither seek, nor act upon, these types of reports. If HHS retains the concept of unsuccessful attempts in the definition, it should revise the regulatory text to at most require logging, but not reporting, of such events.

3. Workstation. HHS proposes to include in laptops computer, virtual devices, and mobile devices such as a smart phone or tablet, in the definition of "workstation." HHS explains that clinicians and other workforce members often rely on mobile devices, and thus the reason for their inclusion, without any discussion or consideration of the practical implications. Mobile devices require different management and control approaches than physical workstations, and therefore should not be lumped in with physical workstations. In addition, mobile devices are already tracked in the technology asset inventory, and so this expanded definition could create redundant requirements and inefficiencies. Keeping the categories separate allows for more targeted and effective security management.

4. Technology Asset. HHS proposes to define the term "technology assets" expansively to mean the components of an electronic information system, "including but not limited to hardware, software, electronic media, information and data." We are concerned that this definition is overly broad, and will require the same systems and data to be treated as assets of multiple entities, resulting in duplicative and unnecessarily burdensome requirements. We are particularly concerned about the inclusion of software, information, and data without any type of qualification or limitation. Focusing instead on hardware systems that store relevant data is a more practical approach. We therefore recommend limiting the requirement to "relevant" hardware systems that "store" ePHI.

Finally, there are also numerous terms used throughout the proposed rule without definition, such as "resiliency," "vulnerabilities," "effectiveness," "critical risk," and "high risk," which creates additional uncertainty, especially when these terms are embedded in key definitions. For example, the Department itself notes that there may be questions as to its interpretation of the term "direct management control," which is embedded in the critical definition of "relevant electronic information system," but there is no definition of the term,

Recommendation:

- **OCR should engage with regulated entities and other stakeholders to narrow the scope and add clarity to many of the new and modified definitions to ensure that they are workable and manageable for regulated entities, and to define key terms**

embedded in these definitions and the proposed rule's requirements that are not defined.

C. Flexibility of Approach

The Department states that it is retaining the current flexible approach that allows regulated entities to take into account certain specified factors when determining which security measures to implement to meet the Security Rule standards, but proposes to add a new factor, namely, the effectiveness of the security measure in supporting the resiliency of the regulated entity.

We strongly support the retention of the principles of flexibility and scalability, which are the hallmarks of the current Security Rule, and are in no small measure the reason it has withstood the test of time as well as it has for over two decades. We are concerned that while intending to provide greater clarity, HHS has instead provided much greater specificity, and done so to such an extent that the foundational principles of flexibility and scalability are retained in name only. This specificity includes, among other things, mandating specific time frames for a host of requirements, and specific types of technical controls, such as MFA and encryption of all ePHI at rest, irrespective of the size and nature of the entity, how it uses ePHI, its risk level, or its cyber maturity level. HHS can define the WHAT (i.e., the security standards) and give regulated entities the flexibility to determine the HOW (i.e., the manner and mechanisms by which the standards will be implemented).

We are also concerned that the Department's new focus on the "effectiveness" of security measures could be used to hold regulated entities to an unattainable standard of security. Specifically, we are concerned that without further clarification, the requirement to consider and test for the effectiveness of a security measure could be interpreted to require that the security measure in question must never fails (i.e., be "bulletproof") since otherwise it would be deemed ineffective. This concern is heightened by the Department's rationale for introducing this consideration, namely, to counter the court's finding in *University of Texas M.D. Anderson Cancer Center v. HHS* (''*M.D. Anderson*'')[5] that the current Security Rule does require that a security measure provide "bulletproof" protection. Since no security measure can be "bulletproof" or 100% effective, regulated entities should not be held to this standard, whether directly or indirectly through an implied effectiveness standard. None of the security guidelines or best practices cited by HHS impose such a standard, and the NIST publication[6] cited by the Department in imposing this new factor refers only to how well an entity recovers to an "effective operational posture" after an adverse event. This is a very different, and much narrower, use of and context for, the term "effective," since it is in fact predicated on some type of failure having occurred, and focuses instead on the ability to recover from it.

Similarly, HHS states that flexibility and scalability must not be at the expense of "adequate security." However, regulated entities are required to implement "reasonable and appropriate" security measures, not "adequate and effective" measures. Terms such as "adequate" and "effective" could be read to set a very different standard that does not allow for any security incidents, breaches, or other security events since, by definition, the occurrence of any of these would arguably indicate that the implemented security measures were not adequate or effective.

---

[5] *University of Texas M.D. Anderson Cancer Center v. U.S. Department of Health and Human Services*, 985 F.3d 472, 478 (5th Cir. 2021)

[6] Joint Task Force, ''Managing Information Security Risk: Organization, Mission, and Information System View,'' NIST Special Publication 800–39, Appendix B, National Institute of Standards and Technology, U.S. Department of Commerce, p. B–5 (Mar. 2011), https:// nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication800-39.pdf.

We urge HHS to reconsider the imposition of effectiveness requirement. Alternately, if HHS does retain this concept, it should clarify how it will be applied, such providing examples of how regulated entities would evaluate effectiveness, and explicit language stating that effective security measures are not expected to never fail.

Finally, we are concerned that the many new and very specific time frames eliminate flexibility by failing to take into consideration not only the nature and size of the entity, but also the facts, circumstances and precipitating events that trigger a time frame. To the extent HHS determines it is necessary and appropriate to specify certain time frames, we recommend that it convene stakeholder groups to determine more realistic time frames that are consistent with those in other cybersecurity best practices and guidelines.

Recommendations:

- **In order to retain flexibility and scalability, the Department should take a less prescriptive, technology neutral approach .**
- **HHS should eliminate the requirements for safeguards to be "adequate" or "effective" or otherwise, clarify that these terms do not require that the safeguards be "bullet proof," but are adjustable and scalable to align with the regulated entity's risk priorities and risk management program.**
- **HHS should engage with stakeholders to identify realistic and flexible timeframes consistent with other cybersecurity best practices.**

D. Addressable Implementation Specifications

HHS proposes to remove the distinction between ''addressable'' and ''required'' implementation specifications to require regulated entities to comply with both the standards and implementation specifications. HHS states that it is making this change because regulated entities were misinterpreting addressable implementation specifications as being optional. HHS goes on to acknowledge that this proposal would reduce the Security Rule's flexibility, but adds that it would not eliminate all of the Security Rule's flexibility and scalability, but simply clarify where the floor of protection must lie.

We agree that the concept of "addressable" implementation specifications has been misunderstood by some regulated entities, and therefore support the elimination of the term "addressable." We also appreciate HHS statement of intent that this proposal would not eliminate all flexibility and scalability. However, as discussed above, we are concerned that as a practical matter the proposed changes will have this effect. This is not as a result of the removal of the word "addressable," but rather, due to the very specific and detailed new requirements which have only very limited, rigid, and narrow exceptions, each with their own set of conditions.

As discussed further below with respect to specific standards and specifications, we believe this overly prescriptive approach is counterproductive. Cybersecurity is, of necessity, a very dynamic field, and requires the ability to adapt quickly to keep up with changes in technology, the environment, and the latest techniques of cyber criminals. Any regulatory framework that requires regulated entities to implement specific security measures based on the current state of technology and cyber risks is not only likely to become outdated, but not to mention costly, to have to constantly revise and update it to avoid becoming obsolete and, consequently, ineffective.

Instead of the one-size-fits-all approach that pervades the proposed rule, HHS should build on the existing rule's flexible risk-based approach by defining sliding scales for requirements that

consider the risk likelihood and severity, the cyber maturity level or cyber certification level, and the compensating controls related to security requirements. HHS should work with stakeholders to determine which safeguards should be essential and when regulated entities should progress to enhanced security measures.

Recommendations:

- **We support elimination of the term "addressable" because of its potential for misinterpretation, but do not support its replacement with mandatory implementation specifications that lack flexibility and scalability.**
- **HHS should instead consider a framework based on defined characteristics of risk, cyber maturity, and compensating controls. HHS should describe the required controls and allow flexibility in their implementation according to the entity's risk priorities and risk management strategies.**

E. Maintenance Requirements

HHS proposes to add explicit maintenance requirements to certain standards to address concerns that regulated entities may be misinterpreting the current maintenance provision at 45 CFR 164.306(e) by not connecting them to the administrative safeguards under 45 CFR 164.308. The proposed rule would impose undue burdens in several ways. Under the proposal, a regulated entity would be required to review and test the measures on a specified cadence, and to modify the measure as reasonable and appropriate. HHS gives as an example of testing written policies and procedures simulating security events that mimic real-world attacks to assess how effectively employees follow incident response and security procedures; conducting knowledge assessments after training on policies and procedures; and reviewing system logs and access records to evaluate whether policies and procedures governing access to ePHI are being followed.

We believe ongoing maintenance of security measures is critical, particularly in light of the rapid advances in technology and changes in the threat environment. We therefore support clarification of the maintenance requirements and their connection to the administrative safeguards to avoid misinterpretation or perceived ambiguity as to how they relate to specific security standards. However, we are concerned that the Department's proposal extends well beyond clarification to include new mandatory requirements to review, test, and modify every security measures at least annually, and potentially more frequently, without any opportunity for regulated entities to prioritize measures or decide whether the proposed maintenance cadence is necessary or appropriate for a particular measure.

This wholesale review and testing and changing of every security measure at least every 12 months or for any operational or environmental change would come at an enormous cost to regulated entities that the Department does not mention, let alone quantify in its regulatory analysis. The Department's example of simulating a security incident alone would be very costly for large regulated entities when considering the preparation, disruption, and loss of work time involved. While such an exercise may well be useful and even advisable on occasion, it does not come without considerable cost and disruption, and there are likely other less costly and more effective ways to keep security measures current and updated on a regular basis. It is unwise and excessive for the Department to dictate the timing, mechanism and required action across the board for every security measure and every regulated entity. Regulated entities will have no ability to prioritize areas of greatest vulnerability or concern, and scarce cybersecurity resources will be expended going through the motions of reviewing, testing, and modifying security measures that are working satisfactorily.

Maintenance requirements should vary based on risk and the maturity of an entity's cyber security program e.g. using CMMC, HITRUST, or other recognized certification program criteria. For example, a maturity level below 2 may indicate a need for annual attention, whereas a maturity level above 3 may indicate a need for maintenance no more frequently than every three years. Industry standards, such as NIST, and best practices (e.g., Health-ISAC) should be the guiding principles for healthcare organizations to use as resources in developing their maintenance requirements and compliance plans.

We strongly urge the Department to reconsider these overly prescriptive and costly maintenance requirements, which will not only divert scarce cybersecurity resources from where they are most needed, but require regulated entities expend them on activities that the regulated entity knows to be unnecessary and/or redundant. Instead, the Department should retain the current maintenance requirements and simply make clear how they apply to the administrative safeguards to the extent HHS believes this may be misunderstood.

Recommendation:

- **The Department should not finalize the proposed maintenance requirements, which are excessive and overly prescriptive, and should instead clarify how the existing maintenance requirements apply to the administrative safeguards to the extent it believes there is currently some misunderstanding of this by regulated entities.**
- **In developing any new maintenance requirements HHS should base the requirements on a combination of risk levels and cyber maturity or certification levels. For example, a high risk business operation combined with a security program having a low maturity level could be required to conduct more frequent reviews or maintenance.**

F. Administrative Safeguards

1. Technology Asset Inventory and Network Map

As mentioned above in our comments on new and modified definitions, the Department's definition of the term "technology asset" is expansive. While the phrase "all technology assets" makes sense for a full understanding of possible routes of risks and threats, it is not appropriate for the technology asset inventory requirement as it would impose a significant burden by requiring the tracking of every hardware piece, including mobile devices and workstations, as well as software, media, and data. At scale, this will be costly and challenging due to the constantly changing number of assets and deployments.

We are concerned that the proposed network map requirement may be unduly burdensome, and could result in vast and unmanageable network maps as interpreted by HHS. Specifically, HHS gives the example of an offshore business associate that performs claims processing, and states that the technology assets used by the business associate to create, receive, maintain, or transmit ePHI would need to be included in the network map of the covered entity because it affects the confidentiality, availability, and integrity of the covered entity's ePHI. If this is the determining factor, it would seem that the technology assets of virtually all business associates would need to be included in the network map of a covered entity, and vice versa. This would be an enormous and costly operation that would have little, if any, practical utility. The network map should be required to document only boundaries where ePHI enters and exits the regulated entity's relevant electronic information system.

Finally, regulated entities would need considerably more time than the propose compliance period to complete the technology asset inventory and network map due to the large volume of assets included in the scope of this requirement. Similarly, maintenance requirements would become ongoing, drawing resources from other cybersecurity activities to the detriment of an organization's overall cybersecurity posture.

Recommendations:

- **The technology inventory of a regulated entity should be limited to hardware assets of the regulated entity that store ePHI.**
- **The network map should not include technology assets of other regulated entities, only the boundaries where ePHI enters the relevant electronic information systems of the regulated entity.**

2. Patch Management

The proposed rule would require that regulated entities install and update a patch within 15 calendar days of identifying a critical risk, or within 30 days of identifying a high risk (or from when patch becomes available). As with other implementation specifications, there are ongoing maintenance requirements.

We support the requirement to implement a patch management protocol, as this supports the Security Rule requirement for risk management to deter common attack types that exploit known vulnerabilities. However, the proposed timeframes are much shorter than is common or feasible in the industry outside of standard workstations. It is common for patches to require several months of testing prior to being deployed on complex or multi-use systems to ensure they operate as intended and do not have negative operational impacts. In addition, many regulated entities are subject to their vendors' patch release time frame. Even assuming that it was feasible for the regulated entity to deploy a patch within the proposed rule's timeframe, where there are dependencies on third party vendors to certify the patch before it is deployed in the regulated entity's environment to ensure continuity of support, it is very unlikely that a regulated entity or its vendor will be able to meet the timeframes set forth in the proposed rule. Finally, in some cases regulated entities may be contractually prohibited from attempting to patch certain systems, such as on medical devices or equipment. Instead of the proposed approach, each regulated entity should be permitted to set its own parameters for patch management based on their risk profile, patch availability and other relevant factors.

Recommendation:

- **Each regulated entity should be permitted to set its own parameters, including time frames, for patch management based on its own risk analysis, mitigating circumstances, and compensating controls.**

3. Information System Activity Review

The proposed rule requires regulated entities to establish policies and procedures for reviewing and retaining records of activity in relevant electronic information systems by persons and/or technology assets, including audit trails, event logs, firewall logs, system logs, data backup logs, access reports, anti-malware logs, and security incident tracking reports, and to review, test, and update these at least every 12 months.

These proposed information system activity review requirements are overwhelming and unreasonable. Not all systems (including legacy systems) provide for the creation of detailed

transaction logs and when hundreds of thousands of interactions with data occur daily, the ability to identify potential unauthorized activity by authorized users real-time is near impossible. As such this requirement is unduly burdensome, as it will require many regulated entities to transition to new systems, which will create disruptions and increase costs.

HHS should allow regulated entities to continue to use a risk-based approach that would allow them to focus on the most important security related events that would indicate malicious activity or compromise controls. For example, for some regulated entities, it may be sufficient and appropriate to leverage security controls implemented to deter intrusion and strong access management controls, and so omit a full information system activity review.

Recommendation:

- **Regulated entities should be permitted to apply a risk-based approach to determine, based on their own risk analysis, whether and the extent to which to perform information system activity reviews, including substituting documented compensating controls where appropriate.**

4. Workforce Security

HHS proposes that 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, and that a regulated entity must notify another covered entity or business associate within 24 hours after a change or termination of a workforce member's authorization to access ePHI or relevant electronic information system maintained by the other covered entity or business associate.

While regulated entities may aspire to meeting these deadlines in the best case scenario, in most cases they are likely to be impractical and unworkable. Not only is it challenging to determine when the time frame begins, but notification processes vary. Even if automated mechanisms are considered for notification, one hour for termination of access is not feasible since it relies on managers submitting timely terminations in HR systems so that the automation can process removal of access. Challenges also exist where related entities may rely on system reports or other processes to run, as well as with prioritizing terminations for those employees who have access to ePHI over those that may have been terminated earlier but do not have access to ePHI.

Recommendations:

- **The Department should not finalize the proposed one-hour and 24-hour time frames, which would not be workable in most cases.**
- **We recommend that HHS instead require notification "without unreasonable delay" or otherwise engage with industry and standards organizations to develop best practices and appropriate specifications, such " notification of termination to security team."**

5. Information Access Management

As part of the information access management implementation specification, regulated entities would be required to ensure network segmentation, i.e., that relevant electronic information systems are segmented to limit access to ePHI to authorized workstations.

Applying network segmentation to all technology assets, including workstations and devices having access to ePHI would be challenging and costly, even for those regulated entities that have the capability to do it. For many regulated entities is would not be necessary across the board, and for smaller regulated entities such as small health care providers, it would likely not be needed at all. To the extent network segmentation requirements are imposed, they should be based on risk factors such as organizational size, scope, degree of IT infrastructure, cyber security maturity level, and connectivity to other parties.

Recommendation:

- **We recommend that HHS eliminate the requirement for network segmentation or otherwise allow regulated entities the flexibility to determine if and the extent to which it is needed.**

6. Contingency Plan

HHS proposes to require that a regulated entity establish 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.

We agree and support the requirements that all regulated entities have a contingency plan that includes a data backup plan, disaster recovery plan and emergency mode operation plan. We also support the new requirement for regulated entities to perform a criticality analysis to assess the relative criticality of their relevant electronic information systems and technology assets in relevant electronic information systems.

However, restoring an electronic information system within 72 hours after a loss or other event, such as a breach, would in many cases not be feasible. Oftentimes it takes days or potentially even weeks, to complete the investigation into the root cause of the loss or event, before which restoration efforts cannot even begin. Restoration efforts may also have to wait on validating security of the environment (i.e., ensuring the attacker is not present in the system) which can take time but is absolutely necessary prior to restoration. A fixed time frame fails to recognize or take into account these and the many other variables that could impact the restoration time frame. In addition, by specifying this tight time frame, the Department is unintentionally encouraging cyber criminals to make, and incentivizing regulated entities to pay, ransom demands in an attempt to meet the restoration deadline Therefore, instead of a set time frame, we recommend a flexible time frame such as “without unreasonable delay” that would allow regulated entities to perform the necessary tasks that are a precursor to critical system restoration. Alternately, best practices for restoration processes and time frames should be developed by an entity such as CISA based on past experience of cyber events in the health care sector.

Recommendations:

- **HHS should provide a flexible time frame, such as “without unreasonable delay” to allow regulated entities to take the necessary steps, the time frame for which may vary based on the event, before critical systems can be restored.**

7. Compliance Audit

The Department proposes to require that regulated entities perform and document an audit of compliance with each standard and implementation specification at least once every 12 months.

The Department states that the audit does not have to be performed by an external party and that health plans subject to the Employee Retirement Income Security Act of 1974 (ERISA) could potentially meet this requirement by following the Employee Benefits Security Administration (EBSA)'s Cybersecurity Program Best Practices to have an annual third party audit of security controls.

We support the requirement for regulated entities to perform periodic compliance audits of their security controls, consistent with cybersecurity best practices. However, we oppose the requirement to audit each and every standard and implementation specification at least once every 12 months. Even without considering the proposed new maintenance requirements, which would involve performing similar activities towards similar ends also annually, but potentially many times a year, this requirement would be costly and burdensome. But when layered on top of the maintenance requirements, it is duplicative and excessive, and will divert scarce cybersecurity resources from other essential cybersecurity activities.

We urge the Department not to proceed with this requirement or otherwise, at a minimum, to allow regulated entities the flexibility to determine how often and which security controls to audit.

Recommendation:

- **HHS should not proceed with this requirement or otherwise, at a minimum, change it to allow regulated entities the flexibility to determine which security controls to audit and how often to do so.**

8. Business Associate Agreements

HHS proposes to require that regulated entities obtain written verification from their business associates at least once every 12 months that the business associate has deployed required technical controls. This is unrealistic and unworkable. It would require 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, as well as 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. HHS states that this requirement aligns with its CPG that requires regulated entities to identify, assess, and mitigate risks to ePHI used by or disclosed to business associates.

While the Department's CPGs call for contracts with vendors to be used to implement appropriate cybersecurity measures, there is no requirement to obtain an annual verification or certification of technical controls or anything similar. In addition, business associates are already required to contractually agree to comply with the HIPAA Security Rule, including all its technical controls. This is over and above the business associate's direct regulatory obligation to comply with Security Rule's requirements, the failure to do so would subject the business associate to the same penalties for violations as covered entities. It is therefore unclear what additional security is obtained by layering on top of these existing regulatory and contractual obligations an annual verification, which must be supported by a written analysis and certification to each covered entity (or upstream business associate, as applicable). This is particularly the case when one considers that it is proposed in addition to the annual compliance audit that business associates are required to perform, as well as the multiple annual or more frequent reviews and testing of their controls.

Many covered entities contract with hundreds, if not thousands, of business associates, and vice versa, and while the primary burden of performing the analysis and verification would fall on

the business associate, each covered entity too would be involved by being required to seek, obtain, and evaluate the verifications. Requiring all these entities to engage in this additional process of compliance verification, which does not in itself strengthen or advance the technical controls the business associate is already required by regulation and contract to deploy is costly and burdensome. It not only duplicates other compliance requirements, but would divert scarce cybersecurity resources from building cybersecurity resiliency to what would essentially become a costly exercise in checking compliance boxes.

Recommendation:

- **HHS should not proceed with this verification requirement by business associates, which is costly, duplicative, and unduly burdensome.**

G. Physical Safeguards

Technology Asset Controls.
The proposed rule would require policies and procedures to govern the receipt and removal of technology assets into, within, and out of a facility, as well as procedures for the disposal of ePHI and technology assets and the removal of ePHI from media. These policies and procedures would need to be reviewed, tested, and updated at least every 12 months.

We recommend that HHS work with industry stakeholders to discuss a risk-based approach, such as allowing regulated entities to extend the review period over several years. Requiring an annual or more frequent review would require significant resources for entities that lack fundamental asset inventory capabilities.

Recommendation:

- **Regulated entities should be permitted a perform technology asset control reviews over an extended time frame consistent with a risk-based approach.**

H. Technical Safeguards

The proposed requirements for extensive and prescriptive technical safeguards impose significant financial and operational burdens, particularly in the areas of multi-factor authentication (MFA), audit trails, and vulnerability management. We recommend the agency work with industry stakeholder to instead adopt a risk-based approach.

1. Encryption

HHS propose to require encryption of all ePHI in transit and at rest, subject to limited exceptions. HHS states that encryption is built into most software today, and where it is not, there are affordable and easily implemented solutions.

Contrary to HHS' stated assumptions about the ease of implementing and affordability of encryption solutions, there are few situations where encryption can simply be purchased and installed like an off-the-shelf product with minimal cost or effort, and fewer still where it will have no impact on performance. Costs of compliance for encryption at rest differ by the type of system being encrypted. Encrypting all data at rest generally incurs costs associated with implementing and managing encryption solutions, including the purchase of necessary hardware and software, key management systems, and potential performance overhead depending on the encryption method and system load. While many cloud providers may offer low or no cost encryption solutions, not all applications and/or data will be included in a cloud environment, particularly for redundant environments (i.e., data center on prem with parallel backups to the cloud). In addition, not all systems (including legacy systems) are technically

capable of supporting encryption at rest and in transit or allow for forced encryption. As such this requirement is unduly burdensome, as it will require many regulated entities to find and utilize new vendors, hardware, or software, which will create disruptions and increase costs. In many cases, implementing encryption using technology such as transparent data encryption technically addresses the requirement, but does not reduce the risk as any user with logical access is able to view the data in clear text.

We are also concerned that HHS does consider the many ways in which ePHI may be used within a regulated entity, and so how encryption may negatively impact performance. Based on HTI member estimates, regulated entities would need 30-40% more hardware to maintain current system performance, if encryption were required at the application level (which is not clear from the proposal). This in turn would impact implementation and make the proposed rule's compliance timeline especially challenging. Even in the best case scenario where hardware with the required functionality exists to address performance issues, procuring hardware within the proposed compliance period would be infeasible for most large organizations where these types of investments are often budgeted for and scheduled years in advance.

The proposal also does not address or appear to appreciate the complexity of implementing encryption once one moves beyond the storage layer Given the complexity, cost and, in many cases, significant performance issues, we recommend that HHS not mandate encryption at rest, but instead be allowed to determine when it is necessary to encrypt ePHI and have the option to utilize compensating controls to safeguard ePHI, such as access controls and network segmentation as part of their cyber defense.

Recommendation:

- **HHS should not change the existing flexibility for regulated entities to encrypt ePHI at rest based on a regulated entity's risk analysis.**

2. Configuration Management

Among other things, the proposed rule would require regulated entities to deploy technology assets and/or technical controls that protect all of its technology assets in its relevant electronic information systems against malicious software, including but not limited to viruses and ransomware.

Since anti-malware protection software does not exist for all technologies and cannot be deployed on all technologies, we recommend that HHS instead allow regulated entities to focus on risk-based deployment.

Recommendation:

- **HHS should allow regulated entities to focus on risk-based deployment of anti-malware protections.**

3. Audit Trail and System Log Controls

Regulated entities would be required to deploy technology assets and/or technical controls that monitor in real-time all activity in its relevant electronic information systems, identify indications of unauthorized persons or unauthorized activity, and alert workforce members of such indications.

We are concerned that requiring monitoring of "all activity" is very broad and onerous and greatly expands the current monitoring standards, including tracking non-ePHI activities. For

example, using a much more limited risk-based approach, a single health insurer may ingest and analyze approximately 19 billion events per month. Expanding this to apply to "all" activity could cause a reduction in the effectiveness of controls due to excess noise in the system. Instead of the proposed all-encompassing requirement, regulated entities should be permitted to use a risk-based approach to determine the activity to be monitored.

Recommendation:

- **Regulated entities should be permitted to use a risk-based approach to determine which system activity to monitor.**

4. Integrity of ePHI

The proposed rule would require regulated entities to deploy controls to protect ePHI from improper alteration or destruction both at rest and in transit.

Clinical information is a living, breathing record that must be regularly amended to remain accurate and relevant as a patient's diagnosis, treatment and medications change. As such, it is infeasible for a regulated entity that is a health care provider to detect if any alteration to PHI done by a workforce member or a business associate is improper. Patients have the right to correct any potential discrepancies when identified.

Recommendation:

- **Regulated entities should be permitted to continue to use a risk-based approach to implement the mechanism most appropriate to protect the integrity of the data within its environment.**

5. Multi-Factor Authentication (MFA)

HHS proposes to require MFA for all technology assets in relevant electronic information systems to verify user identity and for any action that changes a user's privileges, subject to limited exceptions.

While MFA is an industry-accepted standard, it should not be required universally. This would require that all workforce members utilize their personal mobile device or otherwise the regulated entity would have to incur the significant expense of acquiring and distributing authentication tools, hardware tokens or biometric systems. While this may be manageable for workforce members accessing the system remotely, this is unreasonably burdensome and costly when applied to all workforce members. In a retail setting, MFA will cause a disruption in workflow by requiring workforce members to engage in additional steps to login and can cause disruptions and delays if the workforce member loses their hardware token or there are errors with the biometric system. Similarly, in a hospital or clinic setting, where staff may need to sign-in multiple times a day, it would greatly impede their ability to perform their job duties (e.g., nurses may sign-in 50 times or more per shift). Also, by being physically present in a facility, a person would have to establish some level of identity either through badge access or working in a restricted area with other co-workers who would easily identify an unauthorized person. Given the nuances, complexity, and costs of applying MFA across an entire enterprise, especially at server and sub-system levels, regulated entities should be allowed to adopt a risk-based approach to ensure that MFA requirements are both practical and effective, minimizing unnecessary burdens while maintaining robust security measures. For example, some entities may limit MFA to administrative users, given their greater privileges and so higher potential risk, whereas other entities may require MFA for remote network access only.

Finally, we caution against proposing such a specific type of technology solution, which runs counter to the technology-neutral approach of the Security Rule. There is sound reason for this long-standing approach, since what may be considered a state-of-the art solution today could quickly become obsolete in light of the rapid changes in technology.

Recommendation:

- **HHS should give regulated entities the flexibility to apply a risk-based approach to MFA that is practical and cost-effective, such as requiring MFA for administrative users only or for remote network access only, when other security and access controls are in place.**

6. Vulnerability Management

The proposed rule would require regulated entities to identify and address technical vulnerabilities in their relevant electronic information systems, including through automated vulnerability scans, monitoring, penetration testing and patch installation and updates.

The proposed requirement could be interpreted very broadly, particularly with respect to penetration testing of the external-facing network components. Additionally, conducting penetration tests on live systems can pose security and integrity risks. We recommend that regulated entities be permitted to conduct tests in a controlled environment to prevent disruptions and enhance system protection.

Recommendation:

- **HHS should engage with stakeholders to develop penetration testing requirements with more flexible time frames, and define different tests with different purposes and methodologies as part of a risk management program.**

7. Data Backup and Recovery

The proposed rule would, among other things, require regulated entities to deploy technical controls to (1) create and maintain exact retrievable copies of ePHI with such frequency to ensure retrievable copies are no more than 48 hours older than the ePHI maintained in the relevant electronic information systems, (2) monitor in real-time to identify failures and errors, It would also require regulated entities to deploy technical controls to create and maintain backups of relevant electronic information systems and review and test the effectiveness of these technical controls at least once every 6 months.

While we support requirements for data backup and recovery to support business continuity after an event or incident, we have concerns with the requirement that backup data be no more than 48-hours “old.” We are also concerned about requiring effectiveness testing of backups and documenting results at least monthly.

An organization’s data backup policies and procedures set the duration to make copies of production data according to risks and priorities that drive Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) to meet the entity’s business mission. Imposing a 48-hour timeframe is arbitrary and would make it difficult to comply.

Data backup policies and procedures also spell out requirements to check for failure points in the process. While the industry best practice is monthly data restoration testing, entities may decide to test every 2 months, or quarterly, based on risk assessments that best reflect organizational

needs. The added operational cost and workforce fatigue associated with a mandatory monthly backup test frequency outweighs the benefit.

Flexibility can help ensure backup reliability, proactive issue resolution, and recovery confidence. As such, we strongly recommend removing the timeframe requirement of 48 hours for data backup and the required monthly restoration testing. Regulated entities should determine these 2 "time-bound" criteria based on risks and priorities.

Recommendation:

- **HHS should remove the 48 hour time frame for data backup and the required monthly restoration testing, and instead allow regulated entities to determine these time frames**, based on risk assessments that best reflect organizational needs.

I. Organizational Requirements

1. Business Associate Contracts

In addition to existing business associate agreement requirements and the proposed new requirements regarding verification of technical controls, the proposed rule would require that business associate agreements provide that the business associate will report its activation of a contingency plan without unreasonable delay and in no event later than 24 hours after activation.

We are concerned that requiring reporting of activation of a contingency plan, particularly within 24 hours, is overly prescriptive and will not only result in over-reporting, but will draw business associate resources away from addressing the issue precipitating the activation of the contingency plan. Business associates will not have time to assess the seriousness of an event or whether it is transient in nature, and so may report events that are quickly resolved, such as outages that are relatively common. In addition, business associates are already required to report breaches, impermissible uses and disclosures of PHI and security incidents, which are the same types of events that would result in the activation of a contingency plan, resulting in duplicative reporting when the event warrants reporting.

As stated above in our discussion of the Security Rule definitions, if the definition of a "security incident" is not modified to exclude failed attempts, we ask that HHS at least limit reporting by business associates to successful security incidents. Reporting failed attempts is neither practical nor beneficial.

Recommendation:

- **HHS should not require business associates to report the activation of their contingency plan or the occurrence of unsuccessful security incidents.**

2. Group Health Plan

The proposed rule would require that a group health plan's plan document be revised to require that plan sponsors that have access to ePHI implement administrative, technical, and physical safeguards in accordance with the HIPAA Security Rule.

While we appreciate HHS's commitment to safeguarding ePHI, we are concerned the proposal may exceed HHS's regulatory authority and present substantial compliance challenges. In addition, we are concerned that group health plans will be held responsible for their plan sponsor(s) compliance with the Security Rule. To avoid this, if the requirement is retained, HHS

should also include explicit language stating that the group health plan is not responsible for the plan sponsor's compliance. We also ask that HHS make clear that this requirement applies only if the plan sponsor receives ePHI to perform plan administration functions on behalf of the plan, and not if the plan sponsor receives only limited PHI as permitted by 45 CFR 164.504(f)

Recommendation:

- **HHS should reconsider the addition of the proposed language to the plan documents, particularly because group health plans are not in a position to enforce it. Instead, the final rule should provide that that group health plans simply communicate the requirement to protect ePHI confidentiality, integrity, and availability to the plan sponsor(s) by reference to the Security Rule, but should clarify that the group health plan does have liability for any non-compliance with the HIPAA Security Rule by the plan sponsor.**

3. Documentation

The proposed rule includes extensive documentation requirements, including but not limited to documenting policies and procedures, explaining how the regulated entity considered the factors required to be considered in choosing its security measures (e.g., costs, risks, effectiveness), and then every action, activity or assessment required. This documentation must be updated at least once every 12 months.

We support appropriate documentation of security controls, but are concerned that the proposed rule goes too far, both in what must be documented and how often. While regulated entities are, as a practical matter, likely to have some documentation reflecting their consideration of various factors in choosing appropriate security controls, it is not clear what is to be gained by making this a formal requirement, and there is a risk that it will cause regulated entities to place an undue emphasis on formal paperwork at the expense of choosing and implementing appropriate controls. Similarly, regulated entities should not be required to update documentation on a rigid schedule, but should instead be permitted to do so as changes are made to the entity's cybersecurity program based on risk and the maturity level of the entity's cyber security program using CMMC, HITRUST, ISO, or other recognized certification program criteria. For example, a maturity level below 2 may indicate a need for annual attention, whereas a maturity level above 3 may indicate a need for policies and procedures to be reviewed and, if needed, updated, no more frequently than every three years.

Recommendation:

- **HHS should avoid excessive documentation requirements.**
- **Requirements for documentation updates should be based on a regulated entity's risk level, maturity level, and overall security program.**

J. Transition Provisions for Business Associate Agreements

Under the proposed rule, regulated entities would be permitted to continue operating under existing business associate agreements or other written arrangements until the earlier of either the date the contract is renewed on or after the compliance date of the final rule, or a year after the final rule's effective date. This transition period would apply if the existing agreements complied with the Security Rule before the final rule's effective date and are not renewed or modified between the effective and compliance dates.

While we appreciate the Department providing a transition period to update business associate agreement, the proposed timeframe is too short and demands substantial resources. Many regulated entities will have hundreds, if not thousands of contracts that need to be amended.

Even if the amendments are limited to adding only the required regulatory language completing this process within a year is not feasible. However, in many cases, once the contract is opened the parties renegotiate or add other terms or seek to adjust business terms to take into account the new regulatory burden, and this process can take weeks or even months for a single contract. In light of this, we recommend that if the Department retains the requirement to amend business associate agreements, it allow entities until the next time the contract is renewed or amended to make the required changes.

Recommendation:

- **If HHS requires that business associate agreements be amended, it should permit regulated entities to do so at the time the contract is renewed or amended, rather than limit this to one year after the compliance date.**

K. Regulatory Impact Analysis

The Department states that it estimates first-year quantifiable costs attributable to the proposed rule at approximately $9 billion in total, and that it estimates recurring compliance activity costs for years two through five to be approximately $6 billion. The Department adds that it recognizes that some costs may not be quantifiable, such as the cost of preparing technology asset inventories or testing safeguards as part of reviewing and updating policies and procedures and technical controls. The Department also states that the changes in the proposed rule would not substantially change the obligations of regulated entities, but at the same time postulates that the enhanced security posture of regulated entities as a result of the proposed rule would likely reduce breaches so that the proposed rule "would pay for itself."

We strongly disagree with the Department's assertion that the changes in the proposed rule would not substantially change the obligations of regulated entities. On the contrary, the proposed changes would impose significant new requirements on regulated entities at considerable administrative and financial cost. These include new requirements to review, test and update measures at least every 12 months, perform a technology asset inventory of every technology asset and network map including technology assets of other regulated entities, encryption of ePHI at rest, multi-factor authentication (MFA) internally and externally, the ability to reproduce exact copies of data within 72 hours of a loss, new workforce security and training requirements, revising business associate agreements and plan documents, and developing and implementing new and revised policies and procedures, to name only a few. The regulatory impact analysis vastly underestimates these costs, not only the one-time costs, but even more importantly, the ongoing compliance and maintenance costs. For example, it estimates that it would take 2 hours for a regulated entity to conduct an annual compliance audit, 1 hour to update business associate agreement, and less than 5 minutes for a business associate to obtain annual verification of technical controls from a subcontractor. These estimates are patently absurd on their face and orders of magnitude below the time that will be required to implement these requirements. In addition, the Department makes unsupported assumptions to further lower the burden estimate, such as that business associates engage fewer subcontractors than covered entities engage business associates. Without a complete and closer estimate of the costs, it is not possible to perform any kind of cost-benefit analysis to determine whether the cost of the proposals outweigh their real or even perceived benefits, or whether there are less costly, more effective mechanisms for achieving the Department's goals.

We also strongly dispute the Department's assumptions that its proposed changes will reduce breaches such that the proposed rule pays for itself. Even if the Department provided some data to support its speculation regarding breach numbers, the novel theory is flawed in that it relies on the absence of theoretical future costs to pay for real and actual costs that regulated entities

will incur to implement the proposed mandates. We urge the Department to remove this unsupported line of argument and focus instead on the real and actual costs that its proposed measures will require regulated entities to incur.

Recommendation:

- **HHS should reconsider its regulatory impact analysis. It should include all the one-time and ongoing costs of compliance, since the regulatory impact analysis grossly underestimates both the one-time and ongoing implementation costs of the proposed rule.**

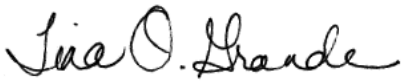
L. Request for Information on New and Emerging Technologies

We recommend that the Department issue separate requests for information on quantum computing, artificial intelligence, and virtual and augmented reality so that stakeholders have the time to focus on providing input on these important topics. We also encourage HHS to maintain and develop partnerships with various agencies as it considers the cybersecurity risks associated with these new and emerging technologies. In particular, we recommend that HHS coordinate with NIST to further develop consensus-based cybersecurity guidelines as part of the AI RMF iterative updates.

HTI appreciates the efforts of HHS to improve cybersecurity in the health care sector through the implementation of more specific and clearer security standards that are effective, workable, and scalable for health care organizations, and our members stand ready to participate and assist in achieving these goals.

Thank you for your consideration of our comments. Please do not hesitate to contact me at tina@hctrustinst.com or 202-750-1989 if you have any questions

Sincerely,



Tina O. Grande
President, Healthcare Trust Institute