Robert F. Kennedy Jr.
Secretary
U.S. Department of Health and Human Services
Washington, DC 20201

Dear Secretary Kennedy,

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments to the Notice of Proposed Rule Making (NPRM) regarding HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information (RIN 0945-AA22.) HIMSS appreciates the opportunity to leverage HIMSS's members' expertise to share feedback on the changes in industry and the appropriate policy levers for protecting electronic protected health information (ePHI). HIMSS's comments reflect HIMSS's public policy principles and the perspectives of a diverse membership.

HIMSS is a global advisor and thought leader and member-based society committed to reforming the global health ecosystem through the power of information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, healthcare leaders, and influencers on best practices in health information and technology driven by health equity. Through HIMSS's innovation engine, HIMSS delivers key insights, education, and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East, and Asia Pacific. HIMSS members include more than 125,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations. HIMSS Americas headquarters are in Chicago, Illinois and global headquarters are in Rotterdam, Netherlands.

HIMSS proposal: An Alternative Approach to Updating the HIPAA Security Rule

Protecting the confidentiality, integrity, and availability of patient information and other sensitive information and assets of stakeholders is a critical component to ensuring the effective delivery and coordination of patient care. HIMSS supports an unified approach to health cybersecurity and information privacy achieved through the creation and adoption of consensus-based and industry-led guidelines, best practices, methodologies, procedures, and processes with use cases and implementation guidance that is scalable for a wide range of healthcare organizations.

At a fundamental level, HIMSS supports many of the measures in the proposed regulation to protect security, such as multi-factor authentication (MFA), encryption, patch management, and security incident reporting, that were in the proposed rule as appropriate best practices. Our concern is the proposal is too prescriptive and not scalable according to diverse levels of resources and risk of the wide range of functions and sizes of regulated entities. Many regulated entities, especially smaller facilities, tribal organizations, post-acute care facilities, and their business associates (BAs), will face significant challenges meeting the proposed rule requirements. The security measure and documentation requirements are overly administratively and financially burdensome and prescriptive. The level of prescriptiveness for how regulated entities must implement and document those actions is simply not necessary to protect ePHI. Also, the cost of compliance with the proposed measures may be significantly higher than HHS estimates, based on the level of prescriptive requirements. The security and risk assessment needs to appropriately protect ePHI will range widely from a large health system to a single provider practice. This proposed rule is a one-size-fits all solution that does not fit the actual risk level as well as capabilities of many regulated entities.

HIMSS believes that cybersecurity requirements should apply best practices, based on level of risk, and be scalable for different sizes and types of regulated entities. Barriers to health information exchange should be minimized by harmonizing security laws, regulations, directives, and industry-led guidelines that are standardized across the United States. Finally, OCR should clarify that regulated entities cannot use compliance with this rule as a justification for information blocking, unless there are reasons consistent with current information blocking exceptions. HIMSS recommends that any ambiguities in information blocking exceptions need to be clarified in conjunction with any finalized changes to the HIPAA Security Rule.

To create a Security framework that applies scalable requirements to protect ePHI that are appropriate for the risk level and capabilities of all regulated entities, HIMSS recommends OCR consider an alternative approach to this proposed rule. To better understand the security capabilities and levels of risk associated with all sizes and types of regulated entities, HIMSS recommends HHS convene a diverse group comprising of all sizes and types of regulated entities, including business associates, small practices, hospitals and providers who care for rural and underserved populations, and long term/post-acute care facilities to identify the appropriate and scalable security, risk management, and auditing requirements. HIMSS believes that the discussion should leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, the HHS Healthcare and Public Health Cybersecurity Performance Goals (CPGs), and the HIMSS 2024 Healthcare Cybersecurity Survey Report as guideposts to frame the discussion. The "Essential Goals" category of the HHS Healthcare and Public Health Cybersecurity Performance Goals (CPGs) provide a more flexible and scalable approach for regulated entities to address highest risk threats to ePHI. The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 also features well received guidelines for communicating risk and developing a cybersecurity program and the controls to address risk. The 2024 HIMSS Healthcare Cybersecurity Survey Report will provide regulators and regulated entities a comprehensive analysis of current cybersecurity practices and capabilities, challenges, and trends across the breadth of all regulated entities to help frame the conversation. These critical conversations would drive meaningful guidance that would enhance security, while scaling appropriately to all regulated entities. Finally, HIMSS recommends leveraging the Health Industry Cybersecurity Practices as part of the conversation. HICP has been developed collaboratively by the Health Sector Coordinating Council Cybersecurity Working Group with HHS and industry partners. HIMSS is a partner is this HSSC collaboration.

In addition, HIMSS recommends the federal government provide targeted support to help regulated entities meet the proposed requirements, through funding, expertise, and comprehensive technical guidance. HHS should also leverage the authority provided by Congress in the 2023 Consolidated Appropriations Act to allow increased flexibilities for large, well-resourced regulated entities to provide tools and resources to smaller, more poorly resourced regulated entities to aid with Security Rule compliance.

Finally, any changes to HIPAA Security Rule compliance requirements need an appropriate implementation period for adoption to ensure a safe transition. The proposed 240-day timeline between the publication of the Final Rule and implementation completion is too aggressive for many regulated entities. The proposed timeline to be compliant following the publication of the Final Rule isn't consistent with industry realities for implementing new compliance processes and ensuring they are appropriately field tested before going live. Therefore, HIMSS recommends a phased implementation timeline, where the requirements for the highest risk activities take priority, to allow regulated entities to safely and appropriately implement the new required measures. As such, HIMSS recommends any finalized changes to the HIPAA Security Rule, should not go into effect until at minimum eighteen months following the publication of the Final Rule.

Observations and Recommendations Related to the Specific Proposals in the Security Proposed Rule

If HHS chooses not to adopt the above proposed alternative approach to the structure proposed in the rulemaking, HIMSS makes the following recommendations and observations regarding the compliance requirements in the proposed rule:

Definition Changes

HIMSS appreciates OCR's consideration to revise definitions to align with new technologies in the healthcare ecosystem. However, the expanded scope and prescriptiveness of some of the revised definitions create barriers to implementation. HIMSS recommends OCR incorporate scalability to some of the definitions, such as risk and technical controls. Regulated entities employ a wide variety of tools and resources to address security, and larger organizations with more resources may be able to apply more advanced technical controls than smaller organizations with fewer resources. As mentioned above, HHS should also leverage the authority provided by Congress in the 2023 Consolidated Appropriations Act to allow increased flexibilities for large, well-resourced regulated entities to provide tools and resources to smaller, more poorly resourced regulated entities to aid with Security Rule compliance.

The **"workstation"** definition has broadened to include not only laptops and desktops but also servers, mobile devices, virtual devices, and medical devices that interact with or store ePHI. The expanded definition scope raises concerns about the increased administrative and financial burdens of maintaining technology asset inventories and the documentation requirements. Also, this definition should distinguish between physical and virtual workstations; some of the requirements apply to both, when requirements apply to either physical *or* virtual workstations.

The definition of **"Electronic Media"** has been proposed to include any digital media or storage used to record, maintain, or process data, except for handwritten data on paper. This broader scope may increase the complexity of compliance, especially with future technologies.

The proposed definition for **"technology asset"** includes all components of an electronic information system, including hardware, software, electronic media, and data. Entities must document and maintain an inventory of these assets and update it annually or more frequently if changes impact ePHI management. HIMSS's members shared concerns about the practicality and cost of implementation with this definition as well as the increased costs of having the effect of diminishing resources available for direct patient care. The increased need for technology asset inventories and tracking could raise the administrative burden, particularly for smaller organizations or those with extensive networks of devices. While HIMSS recognizes the benefit to maintaining a detailed technology asset inventory, the time and cost of doing so outweighs the benefits and the similar security benefits can be achieved through a less granular analysis of categories of technology assets.

The proposed definition of **"security incident"** continues to include "unsuccessful attempts". It has long been, and continues to be, impractical for a business associate to report every unsuccessful attempt, even at an aggregate level. Such a reporting requirement creates a substantial burden and offers minimal benefit. In addition, the requirement for regulated entities to document a response to every unsuccessful attempt is overly burdensome. Finally, the new requirement to "eradicate" all suspected or known security incidents is unclear with respect to unsuccessful attempts – it is infeasible to eradicate all known unsuccessful attempts.

HIMSS recommends that OCR exclude "unsuccessful attempts" from the definition of "security incident" and instead only require entities to respond to successful attempts. HIMSS notes that the regulations can better address unsuccessful attempts as part of information system activity review, requiring regulated entities to monitor unsuccessful attempts and respond based on risk level. Such a change removes the unnecessary burden of documenting and reporting every unsuccessful attempt.

Proposed Security Measure Changes
If HIMSS's alternative proposal for convening regulated entities to rework the proposed rule is not adopted, HIMSS recommends the following changes to the proposed security measures:

Patch Management
The proposed rule, if finalized, would require prescriptive deadlines for the application of patches to all systems containing ePHI, including critical patches within a set timeframe (15 days) and high-risk patches within 30 days. While HIMSS supports guidelines that call for patches to be applied within an appropriate time frame, guided by the results of a risk assessment, the proposed timelines for conducting risk assessments and rapidly patching will be challenging for resource strapped regulated entities. HIMSS strongly recommends OCR consider more flexible guidelines, using a tiered approach based on level of risk. HIMSS also recommends OCR collaborate with the standards community, developers, and the Assistant Secretary of Technology Policy/Office of the National Coordinator (ASTP/ONC) to develop third party tools for automating the risk assessment and patching process.

Technical Safeguards
HIMSS supports the proposal to remove "addressable" from technical safeguard requirements to clarify that implementing the technical safeguards listed in the eventual final rulemaking are "required." HIMSS recommends that OCR consider a tiered approach for technical safeguards based on risk and organizational resources.

OCR should recognize that by making this revision, some small organizations will find the cost of implementing all "addressable" requirements beyond their technical and financial abilities, resulting in closures of entities now providing healthcare. Consideration should be given to the value of access to healthcare versus some of the safeguards. Accordingly, HIMSS recommends that HHS consider providing resources and technical support to regulated entities facing hardships that provide access for Tribal, underserved, rural, long-term care and other at-risk communities to meet the requirements as proposed. As noted above, HIMSS recommendations for a different approach will be more manageable for these regulated entities.

Encryption and Decryption
HIMSS supports the use of encryption as a security best practice. However, there continue to be limited circumstances – beyond the proposed exceptions – where encryption may not be reasonable and appropriate. For example, the Security Rule should allow a health care provider to send an encrypted text message or email that indicates that the individual has received a secure message and provides a means to access the message. Based on HHS' definition of ePHI, such a communication arguably

is ePHI, since it likely identifies that the individual is a patient or plan member of a particular regulated entity. However, it is not reasonable or even feasible for the initial message – the notification of the arrival of a secure message – to itself be encrypted. Therefore, HIMSS recommends that OCR clarify that a notification of the arrival of a secure message itself does not need to be encrypted.

Additionally, while the proposed rule includes an exception allowing an individual to exercise their right of access to ePHI under § 164.524 through an unencrypted form and format, it does not more generally propose that a regulated entity may agree to an individual's request to receive future communications of ePHI (such as future appointment reminders or test results) through unencrypted communications in accordance with § 164.522(b)). Therefore, HIMSS recommends the final rule adopt a more nuanced approach to encryption requirements that scale to the level of risk associated with the specific setting, type of ePHI, and other factors. For example, the rule could require encryption for certain high-risk identifiers (such as Social Security numbers or financial account numbers) and could require encryption of ePHI that includes specific treatment or diagnostic information unless the individual agrees to unencrypted communications of such ePHI. In contrast, ePHI that merely identifies that someone is a patient or plan member, limited data sets, and certain other lower-risk categories of information would not be subject to mandatory encryption requirements.

Penetration Testing
HIMSS generally supports penetration testing as a best practice for regulated entities to identify potential risks. However, the proposed prescriptive requirement for regulated entities to conduct penetration testing every 12 months is not consistent with best practice. Instead, HIMSS recommends OCR adopt a risk-based approach that scales the need for penetration testing to take place consistent with the regulated entities' level of risk.

HIMSS recommends, based on HIMSS's subject matter expert members guidance, the best practice and appropriate requirement is that penetration testing should be performed when there is a significant change in the technology environment. Examples of a significant change would include when a regulated entity:

- converts to a new electronic health record;
- acquires another health entity/provider practice and their systems are integrated with the regulated entities systems; and/or
- interfaces a new vendor system that will upload/download ePHI from the regulated entities' existing systems.

Multi-Factor Authentication
HIMSS supports the use of multi-factor authentication (MFA) to protect ePHI. However, as discussed above, the proposed scope expansion of the definition of "workstation" creates feasibility challenges with implementation. For example, the proposal would require medical devices to use MFA because they would now be considered a

"workstation" and "technology asset" if those devices are accessing, interpreting, transmitting or connecting with an asset that can access, interpret, transmit ePHI, those devices would require MFA. The cost to accommodate MFA on all devices included in the definition will be sizeable and could, create delays in emergent patient care because there is no "breaking the glass" and multiple attempts will result in "lock outs." Balancing the need for security and delivering life-saving patient care must be taken into consideration.

Business Associate Relationships

HIMSS supports OCR's position that business associates (BAs) need to be more accountable for the protection of ePHI. HIMSS recommends that the regulations, however, reflect a shared responsibility model in which it sometimes falls on a BA's customer to deploy technical controls on the BA's information systems. In past cloud computing guidance, OCR indicated:

> *"Where the contractual agreements between a cloud services provider ("CSP") and customer provide that the customer will control and implement certain security features of the cloud service consistent with the Security Rule, and the customer fails to do so, OCR will consider this factor as important and relevant during any investigation into compliance of either the customer or the CSP. A CSP is not responsible for the compliance failures that are attributable solely to the actions or inactions of the customer, as determined by the facts and circumstances of the particular case."*

HIMSS recommends that OCR incorporate this shared responsibility model into the Security Rule. The BA should only be responsible for deploying technical safeguards that are under its control, and not responsible for technical safeguards it offers but are under the control of its customer. For example, in cloud computing, the cloud provider may provide tools like encryption but rely on the customer to turn on and configure the tools. The cloud provider may not have control of those technical controls. HIMSS recommends that the final rule reflects that a BA must deploy and must provide verification that it has deployed technical controls that are under the BA's control.

Business Associate Verification

To aid with simplifying compliance and administrative burden, HIMSS recommends OCR explicitly permit a BA to post verification for compliance with technical safeguards on a publicly available website that can be referenced in response to individual requests, rather than needing to respond to individual requests with the same compliance documentation.

Written Documentation

The proposed rule includes scores of documentation requirements that would prove extremely burdensome, especially for small healthcare providers with limited resources. Each regulated entity would be required to maintain policies and procedures governing dozens of controls, documentation of implementation of those controls, documentation each year demonstrating review of many of the controls, documentation of monthly testing of backups, and numerous documented artifacts, (a risk analysis, a risk management plan, vulnerability scans, penetration tests, compliance audits, evaluations, contingency plans, etc.). The administrative burden of this volume of documentation outweighs its benefit. Instead, HIMSS recommends that the regulations scale back documentation requirements to a few key policies and a smaller number of key artifacts. Regulated entities should be assessed based on what they have done with respect to implementing information security measures, rather than the number of pages of documentation they have maintained.

Requirements for Health Plans

HIMSS recommends providing more scalable requirements for group health plans in which the group health plan itself, through its plan sponsor, only creates, receives, maintains, or transmits ePHI on a random and infrequent basis. For example, an employer (the plan sponsor) may have a self-funded plan and rely entirely on a third-party administrator (a BA of the group health plan) to handle the day-to-day activities that involve ePHI. The employer may occasionally handle ePHI for infrequent events, such as if an employee seeks assistance with a coverage denial or the privacy officer receives a request for access, amendment, or an accounting of disclosures. It is unreasonable to require the employer to implement every requirement of the Security Rule to address the rare instances in which it handles ePHI.

Instead, it would be sufficient to require that the employer, when administering the group health plan, maintains ePHI on a workstation (such as a network drive) in which the ePHI is encrypted (if it includes diagnosis or treatment information or high-risk identifiers such as social security numbers), is only accessible through MFA, and is only available to persons consistent with minimum necessary requirements.

HIMSS looks forward to discussing these issues in more depth. Please feel free to contact Alana Lerer, Senior Manager of Government Relations at alana.lerer@himss.org with questions or for more information.

Thank you for your consideration.

Sincerely,

Thomas M. Leary

Thomas M. Leary, FHIMSS
Senior Vice President and Head of Government Relations