***Submitted electronically via www.regulations.gov***

Association of
American Medical Colleges
655 K Street, N.W., Suite 100, Washington, D.C. 20001-2399
T 202 828 0400
www.aamc.org

March 7, 2025

Anthony Archeval
Acting Director, Office for Civil Rights
U.S. Department of Health and Human Services
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 (RIN 0945–AA22)***

Dear Acting Director Archeval:

The Association of American Medical Colleges (AAMC or the Association) welcomes this opportunity to comment on the proposed rule titled HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, issued by the Office for Civil Rights (OCR).

The AAMC (Association of American Medical Colleges) is a nonprofit association dedicated to improving the health of people everywhere through medical education, health care, medical research, and community collaborations. Its members are all 160 U.S. medical schools accredited by the Liaison Committee on Medical Education; 14 accredited Canadian medical schools; nearly 500 academic health systems and teaching hospitals, including Department of Veterans Affairs medical centers; and more than 70 academic societies. Through these institutions and organizations, the AAMC leads and serves America's medical schools, academic health systems and teaching hospitals, and the millions of individuals across academic medicine, including more than 201,000 full-time faculty members, 97,000 medical students, 158,000 resident physicians, and 60,000 graduate students and postdoctoral researchers in the biomedical sciences. Following a 2022 merger, the Alliance of Academic Health Centers International broadened participation in the AAMC by 70 international academic health centers throughout five regional offices across the globe.

The AAMC shares OCR's commitment to protecting the privacy and security of individuals' protected health information (PHI). Ensuring the security of electronic PHI (ePHI) through the safeguards in the HIPAA Security Rule is critically important in preserving patient access to timely care, as disruptions caused by cyberattacks affect not only the organizations experiencing the attack but can also disrupt patient care. Academic health systems have led the charge in leveraging health information technology (IT) to improve patient access and deliver high-quality care for all patients, investing in electronic health record system (EHRs), bringing care to their patients through the expansion of telehealth, and adopting technological innovations to support the delivery of high-quality health care for all patients. Academic health systems are committed to ensuring the security of their information systems and the PHI these systems produce, as they realize that cybersecurity is a patient safety and access issue as much as it is about safeguarding the infrastructure and assets of the health system. This commitment to cybersecurity has become more evident in light of recent breaches that have necessitated increased investments. Large

health systems are fortifying their IT security infrastructures and allocating more money to cybersecurity,[1] notwithstanding shortages of qualified cybersecurity professionals and limited financial resources.[2]

While we agree with the need for data security safeguards, we believe that the approach taken by the previous administration in proposing sweeping changes to the Security Rule was misguided, lacked a consensus-driven approach to consider feedback from all stakeholders, and grossly underestimated the costs associated with implementing the new safeguards. To that end, we call on the Trump administration to withdraw the above-captioned proposed rule[3] and work collaboratively with stakeholders to put forth requirements that will advance the shared goals of the administration and the private sector to protect patients' health information and prevent costly disruptions to the health care ecosystem. The following summary reflects the AAMC's key recommendations for improving the provisions of the proposed rule that can be used in any future rulemaking to revise the Security Rule:

- ***Collaboration with Stakeholders***: Withdraw the proposed rule and convene stakeholders to further shared goals of advancing cybersecurity.
- ***Compliance Timelines***: Increase timelines for compliance to provide a glidepath for regulated entities.
- ***Standards Alignment***: Ensure alignment with prevailing industry-accepted standards.
- ***Addressable Implementation Specifications:*** Provide flexibility for regulated entities to tailor policies and procedures to correspond to their risk analyses.
- ***Network Map and Asset Inventory***: Allow for a high-level network map and asset inventory.
- ***Network Segmentation***: Provide additional detail on network segmentation requirement, such as types of systems and technology to which the segmentation requirement applies.
- ***Encryption***: Allow additional exceptions to encryption and decryption standard.
- ***Business Associates***: Place business associate responsibility for ensuring adherence to technical safeguards on the business associate and not on the covered entity.
- ***Multi-Factor Authentication***: Allow a risk-based approach to multi-factor authentication.
- ***Patch Management***: Extend patch management timelines and allow a risk-based approach that would offer flexibility in patch management to the regulated entity.
- ***Contingency and Disaster Planning***: Replace the 72 hours deadline for systems restoration with a more flexible approach.
- ***Annual Compliance Audits***: Require external auditors to take part in OCR standards reviews.
- ***Workforce Security***: Extend the termination of access timeline for employment arrangements that end voluntarily.

### *Withdraw the Proposed Rule and Convene Stakeholders to Further Shared Goals of Advancing Cybersecurity*

**The Trump administration should withdraw the proposed rule and engage in a deliberative process to enhance the safeguards of the Security Rule.** This process should at a minimum include consulting with key stakeholder groups, conducting a thorough analysis of the costs and benefits of any proposed

[1] Guidehouse. Health Systems Prioritizing Cybersecurity as 2024 IT Budgets Increase. November 20, 2023.
[2] Chief Healthcare Executive. Healthcare Cybersecurity Budgets are Rising, but Workers Are Hard to Find. March 2, 2024.
[3] HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information. 90 FR 898. January 6, 2025.

changes, and ensuring alignment with other industry-accepted standards. These key stakeholder groups should include public and private sector entities in the health care sector, including affected government agencies, representatives from covered entity and business associate groups, health IT software vendors, and medical device manufacturers. The administration could begin by consulting with the Health Sector Coordinating Council Cybersecurity Working Group, an advisory council of more than 420 healthcare public and private sector organizations tasked with providing sector-wide recommendations on cybersecurity best practices. Consulting with cybersecurity experts within HIPAA regulated entities will enable the administration to better understand the realities of regulated entities' operations and security practices, and the true impact these proposals would have on their security programs. The proposed rule would make sweeping changes to the current technical, administrative, and physical safeguards required under the HIPAA Security Rule. To comply with the rule's provisions, regulated entities, including health care providers and health insurance plans, would have to update written policies and procedures, as well as their safeguards. Due to the broad scope of the rule's changes, updating information systems and practices to meet the rule's requirements would involve significant investments of financial resources and staff time. The rule would not only impose onerous requirements on these private sector actors, such as hospital and health insurance plans, but it would require extensive investments of resources by key governmental agencies, including the Centers for Medicare & Medicaid Services (CMS), state Medicaid agencies, and the Veterans Health Administration, all of which are subject to the requirements of the Security Rule. In the regulatory impact section, OCR predicts total annual costs to regulated entities to be over $9 billion. While we believe this a gross underestimate of the actual burden associated with implementing the rule's provisions, even this estimate would impose substantial costs on private and governmental entities. These excessive costs run counter to the Trump administration's stated goals to alleviate unnecessary regulatory burdens and to ensure that the total incremental cost of new regulations be less than zero.[4] Therefore, it would be in the best interests of the administration and all stakeholders to withdraw this rule.

We agree with the urgency of enhancing security practices to tackle the increase in cyberattacks and the corresponding disruptions to patient access and health care provider and payer operations. However, OCR must go about proposing these changes in a way that recognizes the differences in provider types and defers to the risk analyses of the regulated entities in terms of which security measures are most appropriate for them.

The rule expands the types of information systems to which the HIPAA Security Rule would apply, removes the discretion that regulated entities have to tailor security measures to their risk analyses, and introduces multiple technical, complex requirements. **Given the magnitude of the changes, as well as the unrealistic nature of many of the requirements, OCR should withdraw the rule. If OCR chooses to proceed with finalizing the rule or to address the Security Rule in separate rulemaking in the future, we provide additional recommendations below on how the proposals can be improved.**

***Increase Timelines for Compliance to Provide a Glidepath for Regulated Entities***

For most of the rule's provisions, OCR proposes a compliance date of 180 days after the effective date of the final rule, which equates to 240 days after the final rule is published. OCR proposes a longer transition period for updating business associate agreements (BAAs), which would be the earlier of the renewal date of an agreement or one year following the effective final date of the rule. We urge OCR, if it finalizes the

[4] Executive Order 14192. Unleashing Prosperity through Deregulation. 90 FR 9065. February 6, 2025.

rule in its current form, to provide a longer transition period for regulated entities to come into compliance with the rule. The rule would require substantial changes in regulated entities' security practices, hiring of additional staff and external vendors, and updates to their policies and procedures, among other changes. Noncompliance with provisions of the Security Rule can result in civil monetary penalties of up to $500,000 per violation,[5] as well as potential criminal penalties for violations referred to the Department of Justice,[6] or exclusion from the Medicare program.[7] **Given the severe consequences of failing to comply with provisions of the Security Rule, as well as the complexity of the proposed rule's new requirements, OCR should provide at least a two year compliance date for regulated entities.** This would allow time for covered entities to ensure their systems and staff are up to date and compliant with the regulation's changes.

***Ensure Alignment with Prevailing Industry-Accepted Standards***

Regulated entities follow a patchwork of industry-accepted federal and state standards related to data security, including cybersecurity specifically. For example, as OCR notes in the rule, the ASTP/ONC certification criteria for certified electronic health record technology (CEHRT) includes a privacy and security certification framework for health information technology modules. The Department of Health and Human Services has published voluntary healthcare sector-specific cybersecurity performance goals (CPGs) that are based on industry-accepted best practices and guidelines and are broken down into essential and enhanced goals.[8] The National Institute of Standards and Technology (NIST) has issued a cybersecurity-specific framework with guidance on managing cybersecurity risks as well as guidance on protecting controlled unclassified information in nonfederal systems and organizations.[9] This NIST guidance, NIST Technical Series Publication 800-171 (NIST SP 800-171), has been used by healthcare organizations, including providers, to develop procedures for protecting ePHI. Federal agencies have begun to adopt these standards in their own cybersecurity regulations, including the Department of Defense (DoD) and the National Institutes of Health (NIH). DoD has incorporated the requirements of Pub. 800-171 into its Cybersecurity Maturity Model Certification Program, which governs the protection of sensitive information shared by DoD with its contractors and subcontractors.[10] NIH updated its Genomic Data Sharing Policy to require that users of its genomic data ensure their IT systems comply with the NIST SP 800-171. **Given the adoption of NIST SP 800-171 by other federal agencies and the adherence to these standards by private sector entities, OCR should ensure alignment by incorporating these standards into any new cybersecurity requirements, instead of developing new requirements that could conflict with these standards.** By adopting these vetted standards, OCR would ensure consistency in cybersecurity practices by stakeholders across these critical infrastructure sectors.

***Provide Flexibility for Regulated Entities to Tailor Policies and Procedures to Correspond to their Risk Analyses***

Under the Security Rule, regulated entities must comply with standards related to administrative, technical, and physical safeguards, with implementation specifications under each standard detailing how regulated entities can meet the standards. As the rule is currently structured, implementation

[5] 45 CFR 160.404.
[6] HIPAA Enforcement Process. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html.
[7] Medicare Program; Electronic Submission of Medicare Claims. 68 FR 48805. August 15, 2003.
[8] HPH Cybersecurity Performance Goals. https://hhscyber.hhs.gov/performance-goals.html.
[9] NIST SP 800-171. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf
[10] Cybersecurity Maturity Model Certification (CMMC) Program. 89 FR 83092. October 15, 2024.

specifications are divided into required and addressable specifications. Addressable implementation specifications provide regulated entities with flexibility to determine whether a specification is reasonable and appropriate given the regulated entity's environment and the risk profile of the regulated entity. This approach allows a small provider, for example, to determine that a costly mitigation is not warranted by the entity's risk analysis and risk mitigation strategy and thus is not reasonable and appropriate for that regulated entity. This flexibility is critical in accounting for the wide range of regulated entity types that are subject to the Security Rule's provisions—safety net providers, rural providers, large academic health systems, and non-provider covered entities such as clearinghouse and insurance plans. Now, OCR proposes to do away with the flexibility by removing addressable implementation specifications and instead offers a prescriptive, rigid approach that dictates the manner in which all regulated entities should meet a specified standard. **We urge OCR to maintain flexibility in the Security Rule by retaining the addressable and required framework and to allow regulated entities to institute risk-based approaches, so that their security measures are tied to the results of their risk analyses.**

Beyond the removal of the addressable implementation specifications, the proposed rule is rife with examples of OCR mandating a one-size-fits-all approach, such as prescriptive timelines for different requirements, which do not account for the differences in regulated entity types, let alone the differences in the types of threats and the risks posed by these threats. Large academic health systems with limited resources should be given the flexibility to focus on high-risk areas first, such as core systems, applications, and critical infrastructure. In our comments below, we identify other proposed standards where the Security Rule could benefit from flexibility and the tailoring of security measures to a regulated entity's risk analysis.

***Allow for a High-Level Network Map and Asset Inventory***

OCR proposes a new standard under administrative safeguards, which would require regulated entities to create a written technology asset inventory and a network map of electronic information systems and technology assets that may affect the confidentiality, integrity, and availability of ePHI. As part of the asset inventory, a regulated entity would create a written inventory of its assets that contain the identification, version, person accountable, and location of each asset. The network map would illustrate the movement of ePHI throughout the covered entity's or business associate's electronic information systems, including but not limited to how ePHI enters and exits such information systems, and is accessed from outside of such information systems. Regulated entities would be required to update their network maps and asset inventories at least once every 12 months, and more frequently if necessitated by changes in an entity's environment or operations, such as the purchase of new technology assets, upgrading or patching existing assets, or after identifying a newly recognized threat.

While the creation of a network map and asset inventory are laudable goals that can bolster the security of ePHI, the manner in which OCR proposes to apply this new standard is overly restrictive. Related to the network map, OCR notes that the requirement is not limited to a covered entity's electronic information systems but includes assets used by the covered entity's business associate that affect the confidentiality, integrity, or availability of ePHI. Thus, a covered entity would be responsible for mapping the flow of ePHI not only throughout its own systems but throughout the systems of its business associates. Entities would need to establish mechanisms to ensure both their inventories and network maps remain current and are updated to reflect changes in the technology assets used by the regulated entity. Large health systems typically can have up to hundreds of thousands of end points, thousands of interfaces, and hundreds to thousands of third-party business associates. Developing and maintaining a network map that illustrates how all ePHI moves throughout its network, to and from all systems that transmit ePHI would

be extremely difficult, if not impossible, and would be a very large burden on resources. Most network and infrastructure teams already leverage tools to enable the tracking of ePHI on their networks, so it is not clear that the formal network maps proposed by OCR would effectively reduce cyber risk. **Instead of an overly prescriptive network map and inventory requirement, OCR should encourage a high-level inventory and mapping of the flow of ePHI.**

***Provide Additional Detail on Network Segmentation Requirement***

As part of the access control standard, OCR proposes to require regulated entities have written policies and procedures, as well as technical controls, to ensure their relevant electronic information systems are segmented in a reasonable and appropriate manner. Specifically, a regulated entity with multiple, distinct electronic information systems would be required to separate relevant electronic information systems using reasonable and appropriate technical controls. Network segmentation is a physical or virtual division of a network into multiple segments, creating boundaries between the operational and IT networks to reduce risks, such as threats caused by phishing attacks. Network segmentation could protect an entity's systems in the case of a cyberattack, to prevent the lateral movement of a malicious actor who has gained access to one of the systems, such as from a point-of-sale system to an EHR system. Therefore, network segmentation would be beneficial to have as part of a security compliance program. However, OCR does not specify the types of technologies that should be segmented and should provide more specificity on the technologies subject to segmentation. We appreciate that OCR acknowledges that "reasonable and appropriate" network segmentation would depend on the regulated entity's risk analysis and how the entity has implemented its networks and relevant electronic information systems. Deference to a regulated entity's risk analysis is appropriate in these circumstances. **However, the proposal is vague, and we request that OCR provide additional guidance on its expectations for network segmentation, such as which devices and types of technology should be segmented.** In addition to the types of devices that should be segmented, there are different levels of segmentation that an organization could implement. Complete network segmentation would require years to implement across many disciplines, such as network, security, applications, and medical devices, as well as significant investments in technology to facilitate full network segmentation. Because systems and data flows routinely change, network segmentation could cause disruptions to patient care. **We recommend that OCR provide additional details on its expectations for network segmentation.**

Under the access control standard, OCR also proposes a new implementation specification related to separating administrative and increased access privileges. This would require regulated entities to separate user identities from identities used for administrative and other increased access privileges. There are certain circumstances in which the risks associated with a user gaining unauthorized administrative access privileges could be addressed through compensating controls, particularly where a regulated entity purchases licenses per user, such as in the case of Microsoft A5 licenses. **In these circumstances, OCR should allow regulated entities to consider implementing compensating controls to mitigate risks where these controls and appropriate and effective.**

***Allow Additional Exceptions to Encryption and Decryption Standard***

OCR proposes to elevate the encryption and decryption implementation specification to a standard, requiring that all ePHI at rest and in transit be encrypted using prevailing cryptographic standards, subject to four exceptions:

- When a technology asset does not support encryption of ePHI consistent with prevailing cryptographic standards.
- When an individual requests unencrypted data under the HIPAA right of access and the individual has been informed of the risks.
- During an emergency or other occurrence that adversely affects relevant electronic information systems and renders encryption unfeasible.
- For certain FDA-approved medical devices.

We agree that encryption, when applied appropriately and within reason, is necessary to maintain the security and confidentiality of sensitive data. However, the expansive scope of the proposed encryption standard would be extremely difficult for health systems to implement and would disrupt patient care. While OCR proposes an exception for unencrypted data that is requested under the HIPAA right of access, many other types of data could be subject to the encryption requirement, interfering with patient care. This could include calendar appointments, emails, and alerts sent through patient portals. Encrypting these types of communications would reduce the flow of information between clinicians and patients. **OCR should broaden the exception to cover unencrypted communications (when requested by the patient) between a regulated entity and patient that go beyond the designated record set covered by the HIPAA right of access. To ensure the encryption requirement is not stifling patient access or disrupting health care operations, OCR could also add a new exception that covers situations when there is a reasonable likelihood that encryption would disrupt health care operations or services.**

Beyond the patient access implications of the encryption proposal, the proposal would be technically challenging and costly to implement. Regulated entities, and in particular large academic health systems, have thousands of systems and tens of thousands of client devices. Requiring encryption across all these systems would be a monumental undertaking. The difficulties associated with encrypting data in transit are compounded by the lack of widely adopted encryption protocols for data exchange, resulting in many vendors lacking the technical ability to receive or transmit encrypted data. Regarding the requirement that data at rest also be encrypted, the prohibitive costs outweigh the minimal risk of data loss, particularly when data is stored in secure data centers. **The encryption requirement should be a scaled or risk-based approach that applies to data at rest only in high-risk settings, such as mobile devices, laptops, and USB devices.**

***Place Business Associate Responsibility for Ensuring Adherence to Technical Safeguards on the Business Associate and not on the Covered Entity***

OCR proposes changes to covered entity relationships with business associates (BAs), which are contractors or subcontractors that the covered entity engages with to perform certain functions involving the use or disclosure of PHI, such as claims processing vendors, accounting firms, attorneys or law firms, and health care clearinghouses. Covered entities and BAs must enter into contracts, or BAAs. OCR proposes specifically that:

- Covered entities obtain on an annual basis written verifications from BAs or subcontractors that they have implemented necessary technical safeguards and that the BA would comply with the Security Rule.
- BAAs include a provision requiring a BA or subcontractor to report activation of the BA's or subcontractor's contingency plan to the covered entity no later than 24 hours after activation.

We object to the premise that these requirements are necessary to ensure compliance with the Security Rule, because they put the onus of BA compliance on the covered entity and because updating BAAs and receiving the necessary verifications would be overly burdensome for covered entities and their staff. Past experience with updating BAAs, such as in response to changes to the Security Rule made by the Health Information Technology for Economic and Clinical Health (HITECH) Act, suggest that updating these agreements as proposed would be extremely time consuming. Academic health systems typically have thousands or tens of thousands of BAAs in place. Because BAAs are not typically standalone documents but are part of larger contracts that a covered entity has with a BA, updating these BAAs would not be a matter of simply adding a clause pertaining to the BA's activation of a contingency plan. Instead, updating the BAA would require the covered entity and BA to renegotiate the entire contract. OCR estimates that updating the BAAs would require an hour for each regulated entity. We believe that this is a gross underestimate of the actual time that would be required to comply. For example, for an academic health system with 1,000 BAAs in place, we believe a more accurate estimate would be at least one to two hours to update each BAA, meaning that health system would need to dedicate 1,000 to 2,000 hours to update its BAAs. Receiving annual verifications would be similarly cumbersome, requiring at least one hour per BA and an employee responsible for requesting, tracking, reviewing, and storing these verifications.

In addition to the burden imposed on covered entities by these proposals, the proposals are inefficient mechanisms to achieve the policy goal of improved security. Although the proposals appear to be aimed at improving BA compliance with the Security Rule, they do so by putting the legal obligations on covered entities to update their BAAs and obtain the necessary annual verifications. It is unclear which party, the BA or the covered entity, would be liable for failure to obtain timely verifications. **Instead of these proposals, which unnecessarily burden covered entities and shift the compliance responsibility from BAs to covered entities, OCR could consider alternative policies, such as:**

- Requiring BAs to conduct and document a technical safeguards analysis that would have to be shared upon request by OCR or any covered entity that works with the BA.
- Requiring BAs to report activation of their contingency plan directly to any covered entities they serve, instead of requiring that this be incorporated into BAAs. Alternatively, OCR could exempt existing BAAs from the requirement and require only BAAs that are implemented after a future date to include a provision in the BAA on the activation of a contingency plan.

These changes would allow OCR to achieve its policy goals without imposing unnecessary burdens on covered entities.

In addition to these changes, we urge OCR to revise the requirement that a BA must report to the covered entity "any security incident of which it becomes aware, including breaches of unsecured PHI as required by the Breach Notification Rule."[11] The Security Rule defines "security incident" broadly, to include both attempted and successful unauthorized access, use, disclosure, modification, destruction, or interference with information systems. Under this broad definition, the number of security incidents that a regulated entity is exposed to could be more than 1,000 per hour for a large regulated entity, as OCR acknowledges in the rule.[12] Requiring BAs to report such large numbers of unsuccessful events would be burdensome while providing minimal security benefit to either the BA or the covered entity. **Therefore, we urge**

[11] 45 CFR 164.314(a)(2)(C).
[12] 90 FR 981. January 6, 2025.

**OCR to revise this requirement to provide additional discretion to the BA to focus on reporting successful security incidents, as opposed to unsuccessful events as well.**

***Allow a Risk-Based Approach to Multi-Factor Authentication***

As part of the authentication standard, OCR proposes that regulated entities deploy multi-factor authentication (MFA) to all technology assets in their relevant electronic information systems and for any actions that would change a user's privileges in a way that would alter the user's ability to affect the confidentiality, integrity, or availability of ePHI. We support the need for MFA as an additional step in securing information systems and deterring unauthorized access to sensitive data. **However, as with other provisions of the Security Rule, a risk-based approach (instead of an across-the board, enterprise-wide requirement) to implementing MFA that allows regulated entities to prioritize high-risk areas first would be a better use of regulated entities' resources.** Similar to other proposals in the rule, the cost and time required to implement enterprise-wide MFA in large health systems with complex IT infrastructures can be substantial and far surpasses the estimate of 1.5 hours that OCR includes in the impact analysis. The initial implementation of an MFA solution requires significant evaluation and testing to ensure the chosen solution can integrate with existing applications, offer sufficient protections, and minimize potential operational disruptions. The costs of implementing an MFA solution are not limited to the initial selection and implementation process but continue to accrue annually in the form of operational costs. Maintaining and operating an MFA solution requires a team of engineers to support hundreds of integrated applications, perform ongoing maintenance, and to oversee the evaluation and implementation of new features.

In addition to considering the implementation and maintenance costs, we urge OCR to consider that the benefits of MFA in a specific context or for a specific application must be weighed against the risks and compliance costs of MFA, which include usability impacts, such as disruptions to patient care and staff workflows. Impacts to usability, including user frustration with the MFA process, could ultimately result in risk to availability of data without meaningfully reducing risk to confidentiality, which would be counter to the goals of the Security Rule. The additional time involved in requiring user login to a system with MFA equates to lost patient care time, which is particularly concerning in settings where split-second decisions are made, such as emergency departments and trauma centers. These cost and user disruption considerations weigh in favor of a risk-based approach that would permit regulated entities to determine to which systems and in which circumstances MFA should apply. Under a risk-based approach, an organization could incorporate other factors into its risk calculations on the utility of MFA in a given instance, such as the location of the user at the time of the attempted access. This type of risk-based assessment is incorporated in MFA solutions themselves, which allow user-based geolocation to determine if MFA should be enforced. Many organizations have taken the risk-based approach that on-premise care team staff who access systems do not require MFA because it would cause a delay in workflow, while MFA would be more reasonable and appropriate for remote employees. **Therefore, we urge OCR to revise the proposal to allow for a risk-based approach, which would allow regulated entities to focus on systems, applications, and critical infrastructure that pose the greatest risk for unauthorized access.**

***Extend Patch Management Timelines***

Covered entities would be required under the proposed patch management standard to apply patches and update configurations of relevant electronic information systems within a "reasonable and appropriate time period." OCR stipulates that an appropriate time period to patch or update a system would be within

15 calendar days of identifying the need to address a critical risk and within 30 days of identifying the need to address a high risk. We believe these timelines are unnecessarily restrictive and remove the risk-based approach to determining appropriate security measures. Patch management is complex and involves many different teams within an organization, including product, security, and engineering teams. Applying patches requires front end development, testing, and notifications to customers. Patches are usually installed on test platforms, tested, and then scheduled to be deployed in production. Furthermore, prematurely applying an upgrade or a patch can have severe unintended consequences, as was demonstrated by the recent CrowdStrike outage that resulted from a cybersecurity vendor issuing an update to its software hastily, without having conducted the appropriate validation checks. This resulted in widespread outages in IT systems in the aviation, healthcare, and banking sectors, with estimated direct losses totaling more than $5 billion.[13] This example underscores the need for appropriate testing and evaluation of patches and upgrades to ensure they do not have harmful effects on health care operations and patient access. **Instead of predetermined timelines for implementing patches and upgrades, OCR could consider a risk-based approach that would offer flexibility in patch management to the regulated entity based on risk level of the system in question.**

***Replace the 72 Hours Deadline for Systems Restoration with a More Flexible Approach***

As part of the contingency and disaster planning standard, OCR proposes that regulated entities restore critical relevant electronic information systems and data within 72 hours of a loss. **OCR should replace this timeline with a flexible approach that ties restoration timeframes to the size or nature of the disaster.** As recent ransomware attacks have shown, the organization that has been infiltrated first must determine that the threat actor has been neutralized and removed from its environment before it can begin to recover data and systems. Once the organization determines that the threat actor has been removed, the organization must check its systems before putting them back in production and restoring relevant systems. These steps alone can take longer than 72 hours. In the case of the Change Healthcare breach, months passed before all of Change Healthcare's systems were fully restored. **In addition to making response times proportionate to the size or nature of the disaster, for health care providers specifically, OCR could focus on the restoration of operations or services, as opposed to restoration of specific information systems, to allow providers to use workarounds to restore clinical operations and promptly resume patient care.**

***Annual Compliance Audits***

OCR proposes to require regulated entities to conduct and document a compliance audit annually, confirming the entity's compliance with each standard and implementation specification in the Security Rule. The compliance audit requirement would be work intensive and costly, as these audits require the hiring of external auditors and extensive collaboration with the auditors during the audit process. **To improve the usefulness of the annual audits to the regulated entity, OCR should require external auditors to take part in OCR standards reviews to ensure they are performing effective audits that assess and improve organizational processes and compliance with the Security Rule.**

***Workforce Security – Voluntary/Involuntary Terminations***

The proposed rule includes workforce-related provisions, including an updated sanction policy, workforce security measures, and security awareness training. We agree with the need to enhance workforce

[13] CNN. We finally know what caused the global tech outage - and how much it cost. July 24, 2024. https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html

protections, including mandatory security awareness training. However, the proposed workforce security timeline is insufficient, providing only one hour for a regulated entity to terminate an employee's access to ePHI and to relevant electronic information systems. We understand the need to revoke an employee's credentials upon the end of their employment to avoid any unauthorized access to ePHI once their employment ends and support the one-hour requirement for employees whose employment involuntarily ends. **For those employees who end their employment arrangement voluntarily, OCR should extend the deadline for termination of access to the end of the day the arrangement ends.** The security concerns and urgency implicated by an involuntary termination of an employee are not implicated by voluntary terminations.

**CONCLUSION**

Thank you for the opportunity to comment on this proposed rule. To summarize, the AAMC is supportive of cybersecurity safeguards. However, we request that due to the prohibitive costs and short timelines associated with the proposed Security Rule changes, OCR withdraw the proposed rule. In the meantime, we urge OCR to convene a broad range of stakeholders from the regulated entity community to identify improvements to the Security Rule that would align with existing cybersecurity standards. We would be happy to work with OCR on any of the issues discussed or other topics that involve the academic medicine community. If you have questions regarding our comments, please feel free to contact my colleague Shahid Zaman (szaman@aamc.org)

Sincerely,

Jonathan Jaffery, M.D., M.S., M.M.M., F.A.C.P.
Chief Health Care Officer

cc: David Skorton, M.D., AAMC President and Chief Executive Officer