March 7, 2025

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov

Secretary Robert F. Kennedy, Jr.
U.S. Department of Health & Human Services
200 Independence Avenue SW
Washington, DC 20201

RE: HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information [HHS–OCR–0945–AA22]

Dear Secretary Kennedy,

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to comment on the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) Notice of Proposed Rulemaking (NPRM) on the "HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information**,"** as published in the *Federal Register* on January 6, 2025 (Vol. 90, No. 3). We look forward to continuing to be a trusted stakeholder and resource to you and President Trump – and continuing to deepen the long-standing relationship we have shared with HHS.

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs), chief innovation officers (CIOs), chief digital officers (CDOs) and other senior healthcare IT leaders. With more than 3,000 individual members in 58 countries and two U.S. territories and 200 CHIME Foundation healthcare IT business and professional service firm members, CHIME and its three associations provide a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate, exchange best practices, address professional development needs, and advocate for the effective use of information management to improve the health and care in the communities they serve.

Key Recommendations and Takeaways

CHIME strongly urges HHS to consider our request for the rescission of this proposed rule, as finalizing it would further advance the Biden administration's regulatory agenda. Additionally, CHIME spearheaded a joint provider stakeholder letter, co-signed by eight other associations, urging rescission. This letter was

sent to President Trump, as well as to you and your office, on February 17. Our members strongly believe that the combination of the depth and breadth of the proposed requirements on an unreasonable timeline presents significant challenges, and the unfunded mandates associated with this regulation would place an undue financial strain on hospitals and healthcare systems.

It is CHIME's position that the way to help providers improve their cyber posture is to adopt policies that incent them for adopting cyber tools and best practices rather than penalize them for experiencing a cyber incident. **President Trump's law – P.L. 116-321, as referenced later in this letter and notably absent from consideration in this rule, expressly acknowledges and incentivizes the adoption of recognized cybersecurity best practices by healthcare providers and other HIPAA-covered entities.**

By overlooking this statutory framework, the proposed rule fails to account for existing legal provisions that encourage proactive cybersecurity measures, thereby creating potential misalignment with established federal policy. We need to continue with this approach, rather than impose unreasonable mandates. Given these deficiencies, we urge HHS to focus on policies that support flexible, evidence-based security frameworks that align with industry best practices and the rapidly evolving cyber threat landscape.

Our members are deeply committed to making sound investments in cybersecurity resources to protect the patient data they are entrusted to protect. They have been an active partner with HHS in developing a voluntary set of best practices and they are adopting them. **Our members have expressed, however, that the rule as currently constructed, has the very real potential to threaten the financial stability of the American healthcare system, which is already under considerable pressure.**

Despite our belief that the proposal should be rescinded, CHIME believes it is important to offer our detailed comments on this proposed rule – henceforth referred to as "the Security Rule," to offer greater perspective about the current provider landscape, and why we find this proposal so concerning.

The healthcare sector has evolved significantly to help shape, adapt, and adopt technology to support key healthcare goals around the secure exchange of electronic protected health information (ePHI). Throughout our comment letter, we use the terms Healthcare and Public Health (HPH) Sector/our sector, hospitals and healthcare systems, healthcare delivery organizations (HDOs), and providers interchangeably on behalf of our members. **As noted, CHIME represents executive and senior healthcare IT leaders within the HPH Sector – specifically in hospitals, health systems and other healthcare settings.**

As HHS notes in their overview of the proposed rule, "Several entities, including Federal agencies, have published and maintained guidelines, best practices, methodologies, procedures, and processes for protecting the security of sensitive information, including PHI. Some examples of these resources include the National Institute of Standards and

Technology's (NIST's) ''Cybersecurity Framework,''[1] the HHS 405(d) Program's ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,''[2] […] and the Department's ''Cybersecurity Performance Goals'' (CPGs).[3]" **We wish to reiterate that CHIME has publicly supported all of these frameworks and guidelines – including the HHS CPGs.** Thus, we were disappointed that while HHS stated they "considered them in the development of this NPRM […], we do not believe that these documents are sufficiently instructive for regulated entities to help improve their compliance with the Security Rule."

As HHS notes, "E.O.s 12866 and 13563 direct the Department to assess all costs and benefits of available regulatory alternatives and, ***when regulation is necessary, to select regulatory approaches that maximize net benefits*** (including potential economic, environmental, public health and safety, and other advantages; distributive effects; and equity) [emphasis added]." **Taken with the fact that this proposed rule meets the criteria as significant, we are disappointed that HHS' CPGs – which were developed with industry stakeholders and experts – were not meaningfully incorporated into this proposal.**

HHS states in the executive summary of this proposal, "there has been an alarming growth in the number of breaches affecting 500 or more individuals reported to the Department, the overall number of individuals affected by such breaches, and the rampant escalation of cyberattacks using hacking and ransomware. The Department is concerned by the increasing numbers of breaches and other cybersecurity incidents experienced by regulated entities. We are also increasingly concerned by the upward trend in the numbers of individuals affected by such incidents and the magnitude of the potential harms from such incidents."

To be clear – CHIME and our members agree with these statements completely, and share in the Department's concerns. However, based on the deep experience and expertise of our members, we do not believe that the rule as proposed, would decrease the number of breaches, decrease the overall number of individuals affected by these breaches, or provide any meaningful reduction to the escalation of cyberattacks using hacking and ransomware. Further, the investment that would be required to meet these policies, would strip providers' ability to make truly meaningful cybersecurity investments and will drive up the cost of healthcare for everyday Americans.

We believe the following areas are especially important for HHS to consider – especially if the Administration chooses to move forward with this proposed rule:

- CHIME members believe strongly that cybersecurity is patient safety, and regulatory requirements should not jeopardize their core mission of care.

[1] "The NIST Cybersecurity Framework (CSF) 2.0,'' National Institute of Standards and Technology, U.S. Department of Commerce (Feb. 26, 2024), https://doi.org/10.6028/NIST.CSWP.29
[2] ''Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,'' U.S. Department of Health and Human Services and the Healthcare & Public Health Sector Coordinating Council (2023), https://405d.hhs.gov/Documents/ HICP-Main-508.pdf.
[3] ''Cybersecurity Performance Goals,'' U.S. Department of Health and Human Services (Jan. 2024), https://hphcyber.hhs.gov/performance-goals.html.

- We must move away from a mentality that punishes those that have been victimized by malicious actors and criminals.
- The proposed rule imposes significant costs and burden without meaningfully improving security, failing to address evolving cyber threats while reducing efficiency and increasing vulnerability, especially for smaller and rural healthcare providers.
- The proposed rule is extremely inefficient for both the government and the private sector. The complexity and scope of the requirements would necessitate substantial investments in time, resources, and personnel to achieve compliance, diverting attention and funds away from other critical areas.
- Imposing additional regulatory burdens on rural hospitals would have an inadvertent and devastating impact on these providers and the patients they serve.
- This proposal directly conflicts with an existing law, P.L. 116-321, which President Trump passed during his first administration, and was strongly supported by CHIME.

In HHS' "Justification for This Proposed Rulemaking," they note their "concern about the extent to which regulated entities have updated their security measures to adjust to the changes in the healthcare environment and their operations, including new and emerging threats to the confidentiality, integrity, and availability of ePHI." **However – CHIME members are continuously investing in robust data security and cybersecurity and will continue to do so without overly prescriptive, heavy handed, and burdensome regulation.**

When cybercriminals – often operating from hostile nation-states including the People's Republic of China, Iran, and other non-cooperative foreign jurisdictions – target American healthcare providers, we need increased federal support and resources, not additional mandates that divert critical time and funding away from patient care. Critically, these attacks pose an imminent risk to our national defense. Bringing down a hospital or multiple HDOs at once is a risk for the nation and it shakes the confidence and trust of everyday Americans which is precisely what hostile nation states intend – they are looking to exact physical, financial, and psychological harm.

Therefore, we are offering just a few examples of the significant work our members do each and every day to protect their patients' safety, well-being, and data (ePHI) against these relentless and malicious cybercriminals:

- A mid-sized hospital and healthcare system with 14,000 users successfully stops about **250,000 threats each week;**
- A non-profit health system comprising six hospitals with nearly 1,200 beds **successfully blocks 34,501,114 unauthorized network attempts daily;** and
- The largest provider of orthopedic medicine in their state **successfully blocked 27,181,705 connection attempts made from the Internet to their perimeter network firewall during a 24-hour period.**

Detailed Recommendations

The proposed rule states that, "to address concerns about the increasing level of cybercrime, the President has charged Federal agencies with ''establishing and implementing minimum requirements for risk management'' and robustly enforcing those requirements and Federal laws to help manage that risk.[4] We believe that a comprehensive and updated Security Rule is critical to accomplishing these directives and to the Department's effectiveness as the SRMA for the Healthcare and Public Health sector." **CHIME strongly disagrees with the assertion that the proposed rule is necessary to fulfill former President Biden's directive on cybersecurity risk management.**

While we recognize the critical need to address escalating cyber threats, the proposed rule exceeds its intended scope and imposes regulatory burdens that do not align with the principles of effective risk management. The establishment of minimum security requirements must be both evidence-based and operationally feasible, ensuring that they enhance, rather than hinder, the healthcare sector's ability to respond to evolving threats.

Moreover, the Department's role as the Sector Risk Management Agency (SRMA) does not necessitate the promulgation of overly prescriptive regulations that fail to account for the diverse operational realities of healthcare providers. Instead of enhancing cybersecurity resilience, the proposed rule introduces inefficiencies and unintended consequences that could ultimately undermine the sector's security posture. As such, we urge a reconsideration of this regulatory approach in favor of policies that support flexible, risk-based, and outcome-driven security frameworks. **CHIME wishes to reiterate our request for rescission of this proposed rule, as finalizing it would be a continuation of the Biden administration's agenda.**

The reasons we have requested rescission of this proposed rule – especially its impact to the American economy, cannot be overlooked or overstated. The healthcare sector is a significant contributor to the national economy, and the financial burden imposed by these new requirements could have far-reaching consequences. Increased costs for compliance would lead to higher healthcare costs for patients, reduced investment in other critical areas, and devastate patient access – particularly in rural America. We fully expect that small, rural and otherwise under-resourced providers will close if this rule is finalized. The economic ripple effect could extend beyond healthcare, affecting related industries and the broader economy.

Rescinding this proposed rule aligns perfectly with the intent of President Trump's Executive Order (EO), *Unleashing Prosperity Through Deregulation*,[5] which emphasizes

[4] Presidential Memorandum on National Security Memorandum on Critical Infrastructure Security and Resilience, National Security Memorandum/NSM–22, The White House (Apr. 30, 2024), https://www.whitehouse.gov/briefing-room/ presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ (''Critical infrastructure comprises the physical and virtual assets and systems so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety.'').

[5] The White House. (2025, February 5). *Unleashing Prosperity Through Deregulation*. https://www.whitehouse.gov/presidential-actions/2025/01/unleashing-prosperity-through-deregulation/

responsible regulatory budgeting and the elimination of burdensome rules. The EO calls for at least 10 prior regulations to be removed for each new one introduced, ensuring that regulatory costs are effectively managed. **Rescinding this rule would uphold the EO's directive by preventing unnecessary regulatory expansion and allowing for a more strategic, cost-effective approach to cybersecurity policy.**

Further, if this proposal moves forward, we strongly believe that it will stifle innovation in healthcare. The stringent requirements and the rapid implementation timeline could hinder the development and adoption of new technologies and practices that are essential for improving patient care and operational efficiency. The overly stringent requirements and the aggressive implementation timeline create significant barriers to the development, integration, and adoption of emerging technologies that are critical to advancing patient care, streamlining operations, and enhancing cybersecurity resilience. Healthcare organizations, particularly smaller and resource-constrained providers, may be forced to divert already limited funds away from innovation and towards regulatory compliance, ultimately slowing progress in areas such as artificial intelligence, telehealth, advanced data analytics, and interoperability.

Additionally, the rigid regulatory framework may discourage private-sector investment in cutting-edge health IT solutions, as vendors struggle to adapt their products to meet inflexible mandates rather than focusing on security-driven innovation. By imposing prescriptive controls that fail to account for the rapidly evolving cyber threat landscape, this proposal risks locking hospitals and healthcare systems into outdated security models, leaving them less agile in responding to emerging threats.

Instead of fostering a dynamic and forward-thinking cybersecurity environment, this proposed regulation threatens to create stagnation, hindering the healthcare sector's ability to leverage technological advancements that improve both security and patient outcomes.

Furthermore, despite the significant costs associated with the proposed rule, we do not believe it will result in meaningful improvements to security. The proposed measures do not effectively address the evolving cybersecurity threats faced by the healthcare sector, leading to a significant expenditure of resources without commensurate benefits in terms of enhanced security. This regulation would result in slower response times to cyber incidents and decreased overall efficiency, making hospitals and healthcare providers – especially smaller and rural – more vulnerable to attacks, rather than more secure.

Finally, this rule imposes numerous new mandates without acknowledging P.L. 116-321, which President Trump signed into law on January 5, 2021. This law – supported by CHIME – explicitly requires HHS to consider a regulated entity's adoption of recognized security practices when enforcing the Security Rule. Yet, this proposed regulation fails to address or incorporate that legal requirement, directly contradicting existing statute.

Economic Impact on CHIME Members, Patients & the Government

CHIME has significant concerns regarding the cost-estimate HHS has prepared in the regulatory impact analysis (RIA), as directed by under Executive Order (E.O.) 12866, Regulatory Planning and Review, E.O. 13563, Improving Regulation and Regulatory Review, E.O. 14094, Modernizing Regulatory Review, the Regulatory Flexibility Act (RFA), the Unfunded Mandates Reform Act of 1995 (UMRA), and E.O. 13132 on Federalism. As noted: **"This proposed rule, if adopted, would impose mandates that would result in the expenditure by State, local, and Tribal governments, in the aggregate, or by the private sector, of more than $183 million in any one year** [emphasis added]."

In the proposed rule's "Summary of Costs and Benefits," HHS "estimates that the first-year costs attributable to this proposed rule total approximately $9 billion.**"** Additionally, HHS estimates that, "for years two through five, estimated annual costs of approximately $6 billion are attributable to costs of recurring compliance activities." **Based on our members feedback and expertise, we believe that this is still a woefully inadequate estimate – and does not fully account for the significant costs to the federal government. CHIME is deeply concerned that this proposal will constitute a significant burden on mid-sized, small, rural, and under-resourced providers. It is critical that regulations do not inadvertently create overly duplicative requirements, penalize healthcare providers unfairly, and add burden.**

HHS states that: "As a result of the proposed changes in this NPRM, the enhanced security posture of regulated entities would likely reduce the number of breaches of ePHI and mitigate the effects of breaches that nonetheless occur." **We strongly disagree with the assertion that the proposed changes in this NPRM will lead to an enhanced security posture that reduces the frequency and impact of ePHI breaches.**

This proposal further states that HHS has "partially quantified these effects and presents them in a break-even analysis. The break-even analysis estimates that if the proposed changes in the NPRM reduce the number of individuals affected by breaches by 7 to 16 percent, the revised Security Rule would pay for itself. Alternatively, the same cost savings may be achieved by lowering the cost per affected individual's ePHI by 7 percent ($35) to 16 percent ($82), respectively."

The "break-even analysis" presented by HHS is speculative at best, relying on unsubstantiated assumptions rather than empirical evidence demonstrating a direct causal relationship between the proposed regulatory requirements and improved cybersecurity outcomes. Effective cybersecurity risk management is highly dynamic, requiring flexible, risk-based approaches that account for the evolving nature of cyber threats, rather than rigid regulatory mandates that may quickly become outdated. Imposing additional documentation burdens on covered entities not only diverts critical resources away from active threat

mitigation but also creates compliance obligations that do not necessarily enhance security outcomes or reduce risk in a meaningful way.

Furthermore, we believe that this cost-benefit justification is fundamentally flawed. The analysis fails to adequately consider the substantial financial and operational burdens that regulated entities – particularly smaller and rural healthcare providers – will incur in implementing these requirements. The assumption that compliance costs will be offset by a hypothetical reduction in breach impact is both unproven and overly simplistic, neglecting the complexities of real-world cybersecurity risk mitigation. In practice, the proposed rule's prescriptive controls may divert resources away from more effective, tailored security investments, ultimately making healthcare organizations more vulnerable rather than less.

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

CHIME members believe that the impact of this proposal as detailed in the "Summary of Costs and Benefits" is both profoundly deficient and grossly insufficient. The Regulatory Impact Analysis (RIA) contains critical deficiencies that undermine its validity, as evidenced by two specific examples below, which illustrate HHS's failure to accurately assess both the financial and operational burdens imposed on regulated entities. These examples highlight the RIA and corresponding Cost Estimates' glaring shortcomings, demonstrate its reliance on flawed assumptions, unrealistic cost projections, and a fundamental misjudgment of the real-world challenges hospitals and healthcare systems will face in complying with the proposed rule.

Firstly, HHS "estimates that, on average, regulated entities would have an information security analyst spend ***1.5 hours deploying MFA***, as specifically required under proposed 45 CFR 164.312(f)(2)(ii). This would be ***a one-time, first-year burden that includes an average of 30 minutes for a regulated entity to select an MFA solution that allows them to meet the requirements of the proposal without creating workflow disruptions or delays*** [emphasis added]."

We strongly disagree with the Department's cost estimation regarding the deployment of MFA, as required in this proposal. The assertion that an "information security analyst" would require only 1.5 hours to deploy MFA strains credulity – and significantly underestimates the complexity, scope, and operational impact of implementing such security measures across diverse

healthcare environments. This estimation fails to account for critical factors, including infrastructure compatibility, integration with existing identity and access management systems, user training, workflow redesign, and ongoing administrative oversight.

Additionally, the assumption that selecting an MFA solution can be completed within 30 minutes is wholly unrealistic, particularly given the need to ensure compliance with various interoperability, usability, and security considerations. Hospitals and healthcare systems must carefully evaluate MFA solutions to mitigate potential disruptions to clinical workflows, ensure seamless integration with legacy systems, and address patient care continuity – all of which require extensive time and resource investments.

Moreover, the proposed rule does not acknowledge the potential downstream costs associated with user adoption, ongoing maintenance, and troubleshooting, particularly in environments where clinicians and staff must frequently authenticate across multiple applications and devices. The failure to account for these operational realities demonstrates a fundamental misunderstanding of the burdens imposed by this requirement. **For these reasons, CHIME strongly disagrees with this estimation and believe that – at a minimum – a more comprehensive, evidence-based evaluation of the true costs and implications of MFA deployment in healthcare settings is required before moving forward with this proposal.**

Second, in the "Cost Related to Network Segmentation," HHS "believes that most large regulated entities and many medium-sized regulated entities have segmented their information networks to some degree; however, additional actions may be needed to more fully protect ePHI as required under proposed 45 CFR 164.312(a)(2)(vi). Further, small entities may not have been aware of the importance of segmenting networks or taken steps to segment their networks." HHS additionally asserts that the "Department estimates that each regulated entity would spend an average of 4.5 hours to set up network segmentation in the first year of compliance with a final rule (with a low estimate of 4 hours and a high estimate of 5 hours) at the hourly wage of an information security analyst."

CHIME strongly disagrees with the HHS's assessment regarding the time and cost estimates associated with implementing network segmentation required under this proposal. The assertion that regulated entities – regardless of size – could fully implement or enhance network segmentation within an estimated 4.5 hours demonstrates a fundamental misunderstanding of the complexity, scale, and resource-intensive nature of such an undertaking.

Network segmentation is not a simple, one-time configuration; rather, it requires comprehensive planning, architecture redesign, testing, and continuous monitoring to ensure security, interoperability, and minimal disruption to clinical operations. Large and medium-sized entities, even those with some degree of segmentation, must conduct extensive risk assessments, upgrade infrastructure, and implement policies to ensure

compliance – necessary steps that far exceed the HHS's grossly insufficient time estimate.

For small entities, the burden is even greater, as many lack the in-house expertise and financial resources to design, implement, and maintain effective segmentation strategies. The assumption that such organizations could achieve compliance in just a few hours severely underestimates the financial and operational barriers they face, including potential hardware and software upgrades, staff training, and ongoing system maintenance.

Given these significant oversights, the Department's cost analysis is profoundly deficient and fails to reflect the true scope of resources required for meaningful compliance. CHIME urges HHS to – at a minimum – reconsider this estimate based on industry realities and stakeholder input to ensure that regulatory expectations are both accurate and feasible.

HHS "further assumes that in the following years, the burden to maintain the segmented network would be minimal and incorporated into the maintenance requirements." However, the Department continues by asserting that "the ***total first year estimated cost*** of the network segmentation requirement would be ***$983,711,898 […] with a low estimated total of $874,410,576 […] and a high estimate of $1,093,013,220*** […] [emphasis added]." CHIME members strongly disagree with the Department's cost estimate and underlying assumption that the ongoing burden of maintaining a segmented network would be minimal. This assessment fails to account for the significant financial, operational, and technical resources required to properly implement, monitor, and sustain network segmentation in highly complex healthcare environments.

Hospital and healthcare system CIOs and CISOs understand that network segmentation is not a one-time task but an ongoing security practice requiring continuous monitoring, policy updates, integration with evolving clinical and administrative systems, and staff training to prevent operational disruptions. The assumption that compliance costs will be limited to an initial setup, with negligible long-term maintenance expenses, demonstrates a fundamental misunderstanding of the complexities involved in safeguarding ePHI across interconnected hospital and healthcare system networks, cloud environments, and third-party vendor systems.

Furthermore, the estimated cost calculation relies on a wholly understated time commitment of 4 to 5 hours per entity. In reality, segmentation efforts involve extensive risk assessments, architecture redesigns, firewall configurations, and access control policies – all of which require weeks or months of planning, execution, and testing. Healthcare providers must also consider redundancies for failover, compliance with interoperability standards, and mitigation strategies to prevent disruptions to patient care.

Given these substantial omissions, HHS's cost estimate is profoundly deficient and does not reflect the true financial and resource burden this requirement would impose on our members. Before issuing a new proposed rule – or, if HHS decides to move forward with this Biden administration proposal – CHIME urges the Department to reevaluate this analysis using real-world data and direct input from industry experts to ensure an accurate and practical assessment of the regulatory impact.

Further – we wish to reiterate the cost of this proposal to the federal government. As stated in the RIA, "E.O.s 12866 and 13563 direct the Department to assess all costs and benefits of available regulatory alternatives and, ***when regulation is necessary***, ***to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive effects; and equity)***. ***The proposed rule meets the criteria as significant under section 3(f)(1) of E.O. 12866, as amended by E.O. 14094*** [emphasis added]."

As outlined in the RIA:

> ***Each covered entity and business associate (collectively, "regulated entity"), including government entities that meet the definition of covered entity (e.g., State Medicaid agencies)****, would be required to: conduct a Security Rule compliance audit; report to covered entities or business associates, as applicable, upon activation of their contingency plan; deploy multi-factor authentication (MFA) in and penetration testing of relevant electronic information systems; complete network segmentation; disable unused ports and remove extraneous software; update cybersecurity policies and procedures; revise business associate agreements; and update workforce training* [emphasis added].

Further, it is unclear that the total estimates in the proposal's RIA account for the impact on the Centers for Medicare and Medicaid Services (CMS) and the Veterans Health Administration – which is concerning for a myriad of reasons. "The Veterans Health Administration is America's largest integrated health care system, providing care at 1,380 health care facilities, including 170 medical centers and 1,193 outpatient sites of care of varying complexity (VHA outpatient clinics), serving 9.1 million enrolled Veterans each year."[6] Nor does it account for the increased funding that would be needed for OCR – which will need to hire additional staff, provide training and education, and the necessary costs for implementation and oversight of the final regulation.

Finally, the RIA states:

> *Costs for all regulated entities to change their policies and procedures alone would increase costs above the UMRA threshold in one year, and costs of health plan sponsors would increase total costs further. Although Medicaid makes Federal matching funds available for States for certain administrative costs,*

[6] Veterans Health Administration. (n.d.). *VA.gov | Veterans Affairs*. https://www.va.gov/health/

> *these are limited to costs specific to operating the Medicaid program.* ***There are no Federal funds directed at Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance activities*** [emphasis added].

In summary, not only will the costs of this proposed rule be insurmountable for some, but our members will need to address innumerable challenges due to regulatory burden as a result of this proposal. As one of our members shared, they are deeply concerned that this proposal "would implode the American healthcare system." CHIME strongly believes that this proposal will impose a substantial financial burden on our members in terms of passed-on costs from these requirements as well as implementation within their organizations. **Finally, imposing unfunded mandates of this magnitude disproportionately impact some providers in our sector more unevenly – especially rural hospitals and health systems, safety-net, critical access hospitals (CAHs), and long-term and post-acute care providers.**

Hospitals and healthcare systems across the country are already operating on slim margins. Given their limited resources, this proposal would also inadvertently – yet significantly – impact the types of services offered by our members. For instance, while surgical volume may generate revenue, services like behavioral health might not be as financially sustainable. **Thus, an unintended consequence of the additional financial burdens on these already razor-thin margins could be the reduction or elimination of essential services that are critical to the well-being of the communities and patients our members serve.**

CHIME strongly believes that improving cybersecurity will improve healthcare, but reducing financial burden and complexity must take a front seat. As proposed, we are concerned that these policies, while well-intended, will not achieve this goal. Furthermore, it could threaten to upend access to care which is already seeing erosion among some providers due to the aforementioned challenges.

Compliance Deadlines

As proposed – the effective date of a final rule would be 60 days after publication. Regulated entities would have until the "compliance date" to establish and implement policies, procedures, and practices to achieve compliance with any new or modified standards. Except as otherwise provided, 45 CFR 160.105 provides that regulated entities must comply with the applicable new or modified standards or implementation specifications no later than 180 days from the effective date of any such change.

CHIME members strongly believe that this timeframe is impracticable if not impossible for most providers. It does not reflect the operational realities, resource constraints, or technical and administrative complexities inherent in implementing any new or modified regulatory requirements – let alone this specific proposal's regulatory reach and substantive scope. Regulated entities – especially hospitals and healthcare systems, where regulatory frameworks are

inherently complex – require sufficient time to interpret final rulemaking, assess compliance obligations, and integrate those requirements into existing governance structures. The proposed timeframe is insufficient for legal, compliance, and operational teams to conduct the necessary regulatory analysis, draft and approve internal policies, and establish appropriate procedures.

New or revised regulatory mandates often necessitate changes to information systems, vendor contracts, workforce training, and internal audit mechanisms. Many regulated entities must also navigate multi-layered compliance reviews, board approvals, and procurement processes, all of which take significant time. Sixty days does not provide the runway needed for such comprehensive changes, especially for hospitals and healthcare systems, which have sophisticated IT infrastructures. It will be even more challenging for those subject to additional state or contractual requirements.

Historically, regulatory frameworks of comparable complexity have provided compliance windows of six months to two years. For example, HIPAA's Privacy and Security Rules[7] granted covered entities a two-year compliance period, recognizing the substantial investments required to align with new standards. The proposed 60-day window diverges from established regulatory precedent and fails to account for necessary industry-wide implementation efforts.

Compressed compliance windows increase the likelihood of noncompliance, not due to willful disregard, but because of the inherent impossibility of implementing sweeping changes in such a short period. This could lead to enforcement backlogs and potential legal challenges, ultimately undermining the rule's intent. A more reasonable compliance timeline would promote adherence while mitigating unnecessary disruption. To ensure successful implementation without undue burden on regulated entities, HHS should adopt a more feasible compliance timeframe consistent with regulatory best practices. A phased approach of the proposed new requirements would better balance the agency's policy objectives with the operational realities faced by affected stakeholders.

Additional Feedback & Input

While we have outlined some specific concerns regarding the feasibility of the proposed MFA and network segmentation requirements above, our members have identified numerous additional provisions within the proposal that warrant serious consideration due to their potential operational, technical, and financial implications. Below are just a few of them, along with real-world expertise input from our members.

Standard: Encryption and Decryption

HHS proposes that the new standard would require a regulated entity to configure and implement technical controls to encrypt and decrypt all ePHI in a manner that is

[7] U.S. Department of Health and Human Services. (2003). *Health Insurance Reform: Security standards; Final rule*. *Federal Register, 68*(34), 8334-8381. U.S. Department of Health and Human Services. (2000). *Standards for privacy of individually identifiable health information; Final rule*. *Federal Register, 65*(250), 82462-82829.

consistent with prevailing cryptographic standards. Because the prevalence of encryption solutions has increased, as has their affordability and the role they play in protecting information, including ePHI, the Department believes it is appropriate to consider requiring encryption and elevating it from an implementation specification to a standard to increase its visibility and prominence. Based on this and consistent with HHS' HIPAA advisory body, the National Committee on Vital and Heath Statistics' (NCVHS) recommendation, the Department proposes to redesignate the implementation specification for encryption and decryption at 45 CFR 164.312(a)(2)(iv) as a standard at proposed 45 CFR 164.312(b)(1). The proposed standard would incorporate the requirements of two implementation specifications that address encryption—the one addressed here and the one at 45 CFR 164.312(e)(2)(ii).

CHIME members have already taken proactive steps with encryption and decryption and view this proposal as redundant, costly, and operationally burdensome. They are already using robust encryption algorithms to secure ePHI – and believe this proposal would impose duplicative efforts, which leads to inefficiencies and will waste the existing investments they have already made.

Our 2024 Digital Health Most Wired (DHMW) Survey (DHMW) survey revealed that 99% of respondents are already employing encryption at rest (device encryption). The survey encompassed nearly 48,000 facilities, including acute care, ambulatory, and long-term/post-acute care settings. **Therefore, we believe this proposal would unnecessarily escalate costs and operational complexity without providing any significant enhancement to data security, ultimately undermining the value of the substantial encryption investments these facilities have already made.** Additionally, our members' existing systems are designed to be flexible and scalable, and these additional requirements may hinder that adaptability, making them less agile in responding to both internal needs and external cybersecurity threats.

For example – layering encryption in this manner can overcomplicate IT architecture, increasing operational risks and requiring more sophisticated key management systems. Introducing new encryption keys at the server layer, alongside other layers – could actually increase the attack surface for potential breaches, while complicating disaster recovery and access control. Security standards and policies must account for the dynamic nature of cybersecurity threats.

CHIME members believe that by generalizing cybersecurity policies to fit all health IT systems, this proposed new requirement will fall short of its intended goal of making ePHI more secure. Rather, it will inadvertently add new vulnerabilities and increase cost and complexity to mission critical systems required to provide care to patients across the U.S. safely and reliably.

Disaster Recovery Plan

HHS proposes to redesignate the implementation specification for disaster recovering planning. The Department proposes to clarify that a regulated entity would be required to establish (and implement as needed) written procedures to restore both its critical

relevant electronic information systems and data within 72 hours of the loss, and to restore the loss of other relevant electronic information systems and data in accordance with its criticality analysis.

CHIME members believe that this proposal reflects a fundamental misunderstanding of the operational complexities, infrastructure dependencies, and real-world challenges that our members navigate when responding to system outages and cyber incidents. "Disaster recovery" in the healthcare sector is not a one-size-fits-all process; it is a highly intricate and resource-intensive endeavor that depends on numerous variables, including the nature of the disruption (e.g., cyberattack, natural disaster, hardware failure), the scale of affected systems, third-party vendor dependencies, and the availability of secure, uncompromised backup environments. While expeditious recovery is always the goal, imposing an inflexible 72-hour mandate fails to account for the realities of cyber incidents such as ransomware attacks, where forensic analysis, containment measures, and system integrity verification must be prioritized before restoration can safely occur.

Further, we are concerned that the proposed requirement for organizations to demonstrate full recovery from a cybersecurity incident within 72 hours may have the unintended consequence of incentivizing ransomware payments. Imposing such a stringent timeframe could compel entities to prioritize expedient resolution over comprehensive forensic investigation and secure restoration processes. In cases of ransomware attacks, organizations facing an inflexible deadline may determine that paying the ransom is the only viable path to compliance, thereby emboldening threat actors and perpetuating the ransomware economy.

Even in scenarios where uncorrupted backups exist, the requisite forensic analysis—identifying the root cause of the breach, ensuring adversary expulsion, and verifying the integrity of restored systems—cannot be reasonably accomplished within a 72-hour window. This mandate fails to account for the complexity of incident response and system recovery, particularly for large-scale enterprises and government agencies with extensive IT environments.

Accordingly, we urge reconsideration of this requirement, as its operational impracticality does not yield a proportional reduction in cybersecurity risk. Instead, a more risk-informed and flexible approach—one that prioritizes thorough remediation and system integrity over arbitrary recovery timelines—would better serve the overarching goal of strengthening cybersecurity resilience.

Moreover, this requirement does not account for the varying capabilities of healthcare organizations, particularly smaller and rural providers, which may lack the redundant infrastructure, cybersecurity personnel, and financial resources necessary to achieve compliance within such a rigid timeframe. For large, integrated healthcare delivery systems operating across multiple facilities and relying on complex, interconnected systems, a blanket 72-hour restoration mandate could inadvertently introduce security risks if recovery efforts are rushed without adequate validation and testing.

Given these concerns, CHIME urges HHS to reconsider this proposal in favor of a more flexible, risk-based approach that allows healthcare organizations to tailor their disaster recovery plans based on their unique infrastructure, risk assessments, and operational realities. **Imposing an arbitrary recovery timeline could compromise security, patient safety, and the overall resilience of healthcare IT systems.**

The Cybersecurity Landscape and National Security

The Health-ISAC 2025 Health Sector Cyber Threat Landscape[8] highlights a continued escalation of cyberattacks, with the top impact on HDOs reported as: "Disruption in the normal operation of medical technology, including such things as loss of diagnostic technology or loss of access to electronic medical records which may cause delay and disruption to patient care, such as diversion of patients and ambulances, canceled surgeries, or the need to revert to manual procedures."

Hostile nation states have grown increasingly aggressive with their tactics, attacking hospitals and other healthcare stakeholders daily. This poses an imminent risk to our national defense. **Put simply, cybersecurity is national security.**

We urge HHS to take into consideration the increasingly complex cybersecurity landscape hospitals and health systems must navigate. Privacy of healthcare data is not possible without security. Hospitals and healthcare systems are spending an increasing amount of time, energy and resources navigating this highly challenging and evolving environment. **CHIME's 2024 DHMW Survey shows that over the past several years, security has maintained position as the highest priority for digital investment – with 99% of respondents stating that "Security" is essential or high priority. Organizations surveyed are also increasing their financial commitment to information technology (IT), with average budget allocations for IT systems and initiatives nearly doubling year over year.**

HDOs know that is "not if but when" that they will experience a cyberattack. They are no match for well-funded hostile threat actors. Currently, hospitals are also forced to balance the challenges of the high cost of cyber insurance, near-constant cyberattack attempts, the inherent risks to their patients, the weaponization of AI, and the current workforce shortage needed to mitigate all of these risks.

Hospitals and healthcare systems remain lucrative targets for theft and exploitation, particularly through ransomware attacks. Criminal groups and adversarial nation states utilize tactics, techniques and procedures across our sector – including attacking large, publicly traded companies with far greater resources than most U.S. hospitals and health systems. The overall privacy and cybersecurity landscape has become infinitely more complex for all providers.

[8] Annaloro, J. (2025, February 21). *Health-ISAC 2025 Health sector Cyber threat landscape*. Health-ISAC - Health Information Sharing and Analysis Center. https://health-isac.org/health-isac-2025-health-sector-cyber-threat-landscape/

Cybersecurity attacks are on the rise for providers of all sizes which pose a direct threat to patient safety. The costs to recover from a data breach in the Healthcare and Public Health (HPH) Sector are staggering – averaging $10 million per incident, which is far higher than any other sector. As a comparison, the costs for a financial entity to recover from a breach are estimated to be $6 million. Healthcare has held the unfortunate title of top costliest industry for breaches since 2011.[9]

Additionally, the costs of delivering care continue to increase at an unsustainable rate. While all subsectors in healthcare are feeling cost pressures, HDOs are facing:

- Increasing operating costs such as inflation and labor shortages;
- Impact of cybersecurity events such as ransomware and data breaches;
- Continued downward pressure on hospital, physician practice, and smaller HDO reimbursements;
- Supply chain vulnerabilities; and the
- Push from “Fee for Service” to “Value-Based” contracts.[10]

These factors in turn drive increased mergers, acquisitions, & divestitures (MA&D) and consolidation activities; focus on cost reduction; closures / reduced options for health services, especially in rural areas; and an increase in out-of-data / out-of-support vulnerable technologies. Nevertheless, our members undertake and devote significant resources to securing their networks and systems because they are truly committed to the health, well-being, and safety of patients in the communities they serve.

Like nearly all organizations in the United States, hospitals and HDOs must care – to some degree – about their ability to generate positive net revenue in order to keep their doors open. However, they are unlike other organizations in that their first and most important mission is to care for their patients. Hospitals and healthcare systems are not only critical to the communities in which they serve, they are also often the largest employers.

We must continue to move away from a mentality that punishes those that have been victimized by malicious actors and criminals. Cybersecurity is a shared responsibility; however, without additional assistance, many of our members are limited in what they can do.

According to IBM’s Annual Cost of a Data Breach Report 2024: “The average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10 percent spike and the highest increase since the pandemic. A rise in the cost of lost business, including operational downtime and lost customers, and the cost of post-breach responses, such as staffing customer service help desks and paying higher regulatory fines, drove this increase. Taken together, these costs […] [are] the highest combined amount for lost business and post-breach activities over the past 6 years.”[11]

[9] Cost of a data breach 2024 | IBM. (n.d.). https://www.ibm.com/reports/data-breach
[10] Health Sector Coordinating Council. (2024). Health Industry Cybersecurity – Strategic Plan (2024–2029). https://healthsectorcouncil.org/wp-content/uploads/2024/02/Health-Industry-Cybersecurity-Strategic-Plan-2024-2029.pdf
[11] *Cost of a data breach 2024 | IBM*. (n.d.). https://www.ibm.com/reports/data-breach

The IBM Report also found that over "half of breached organizations are facing high levels of security staffing shortages. This issue represents a 26.2 percent increase from the prior year, a situation that corresponded to an average USD 1.76 million more in breach costs. The number of organizations facing a critical lack of skilled security workers rose dramatically, to 53 percent in 2024 compared to 42 percent last year. This year's research found a strong link between the worsening skills shortage and higher data breach costs."

Cybersecurity challenges and threats that our members are facing are what those who have been active in the cybersecurity landscape have known for years – healthcare is under constant threat and more resources are needed for healthcare providers. The budget and resources our members would need to allocate to comply with any new regulations are valuable funds and assets that could otherwise be directed toward critical investments to enhance hospital and healthcare systems' cybersecurity posture and innovation. Any investment in cybersecurity for the healthcare sector will be an investment not just in patient safety – but also national security.

Conclusion

In closing, CHIME appreciates the opportunity to comment on this proposed rule. As previously mentioned – CHIME members are executives and senior healthcare IT leaders – and we are offering to serve as a resource to HHS throughout this process. Our members are extremely knowledgeable and have decades of experience executing cybersecurity best practices, as well as real-world experience dealing with the ramifications of cyberattacks. We look forward to continuing to be a trusted stakeholder and resource to you and continuing to deepen the long-standing relationship we have shared with HHS.

Working together through the rulemaking process is just one way we can accomplish our shared goals and make meaningful changes in cybersecurity and healthcare – because at the end of the day, cyber safety is patient safety. Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Director, Federal Affairs at carnone@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME