



Header Information:

March 7, 2025

The Honorable Robert F. Kennedy Jr.
United States Secretary of Health and Human Services
Centers for Medicare & Medicaid Services
Hubert H. Humphrey Building
200 Independence Avenue, S.W.
Washington, DC 20201

Via electronic submission

RE: 45 CFR Parts 160 and 164: HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Secretary Kennedy:

The Arkansas Hospital Association (AHA) represents over 100 health care facilities and more than 45,000 employees across the state, all of whom are dedicated to delivering essential health care and community services to the people of Arkansas. On behalf of our member hospitals, we appreciate the opportunity to submit comments to the Department of Health and Human Services (DHHS) regarding changes to 45 CFR Parts 160 and 164 titled HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information.

We firmly agree with the overall purpose of the HIPAA rules and the importance of safeguarding sensitive patient data. Arkansas hospitals have a longstanding commitment to the secure handling of such information, continually investing in cybersecurity measures and comprehensive staff training. Robust security rules are essential not only to protect electronic protected health information (ePHI) but also to maintain the public's trust in our health care system – a trust that is fundamental to delivering quality care.

While we support the modernization of the HIPAA Privacy and Security Rules, we are concerned that the extensive changes proposed by previous administrations may prove to be overly detailed and burdensome for hospital entities. In particular, the new reporting requirements and other significant modifications require careful review and time for proper implementation by the incoming administration. **The projected annual cost impact of approximately \$4.655 billion on health care entities further underscores the need for a phased and thoughtful approach to ensure that these changes are both practical and sustainable.**

While we endorse the modernization of HIPAA as a critical step toward enhancing the security of ePHI, **we caution against the potential for adverse financial and patient care outcomes if these proposed rules are enacted**

without adequate safeguards. In the following sections, we provide our detailed comments on the specific changes proposed, outlining both our support for necessary updates and our concerns regarding potential unintended consequences.

Privacy Rule Definitions – Section 160

We believe the proposed modifications in Section 160 accurately capture the current use of electronic media. By expanding the definition to include media on which data may be recorded, maintained, or processed – and by revising the description of transmission media to reflect that data is transmitted almost exclusively in electronic form today – these changes reflect modern practices in health care settings. Furthermore, the revised language is forward-looking and should accommodate future technological innovations, ensuring that new forms of electronic storage or transmission will be covered under the existing framework.

Additionally, the non-exhaustive list of examples the Department provided appears to represent the technologies regularly used by hospitals and health care entities. . Our members remain committed to flexibility in their security practices so that future technologies receive the same level of scrutiny and security measures as those explicitly identified in the current Privacy definitions.

Privacy Rule – Section 164

Proposed Definition and Terminology Changes:

We welcome the Department’s initiative to modernize the Security Rule’s language by updating key definitions. At the same time, we urge caution to ensure that none of the proposed definitions inadvertently impose adverse consequences on regulated entities. Any change introduced has the potential to impact the delivery of care – particularly if barriers in data transmission and access are inadvertently created. While we understand that DHHS must balance the privacy concerns of patient data with the need to promote timely access to critical health care services, the future remains uncertain, and we are unsure of the impact these new definitions will have on novel technology. **We highly recommend that the new administration review its internal plans for the future of health care and collaborate closely with industry leaders, including hospitals and their associations, to ensure these definitions are broad enough to protect patient information while remaining flexible enough to guarantee that patients receive adequate care in a timely manner.**

In particular, we recommend that the Department closely examine the definitions of “information systems” and “electronic information systems” in the context of cloud computing. It is imperative to clearly delineate the extent of control exercised by covered entities versus business associates, especially since the new rules hold regulated entities accountable for the practices of their business associates. While we understand the necessity for these rules, we are concerned about the limited availability of alternative vendors in emerging technology markets. With the advent of innovative technologies, the market can become singular, leaving regulated entities with few options if a current vendor is the sole provider. **If not carefully crafted, these rules could inadvertently hinder the efficient adoption of new technologies in the health care space. We urge DHHS to weigh these issues carefully when finalizing the rule, ensuring that no additional barriers are erected that could slow the pace of health care modernization.**

Additionally, we generally agree with the updated and added definitions; however, we have concerns regarding the long-term applicability of terms such as “implement.” The clarification that implementation requires the technology to function as expected may pose risks during unexpected system downtime. It is important for DHHS to recognize that no technology is perfect, and regulated entities cannot guarantee that the technologies provided by their vendors will be available at all times. **We recommend that DHHS incorporate exceptions for periods when key functions are unavailable due to vendor-related issues, such as contractual limitations with business associates.** This approach would help ensure that the Security Rule remains practical and effective in

real-world scenarios without compromising the intent to protect patient information and provide continuous, high-quality care.

Implementation Specifications and Adaptability:

We understand that DHHS faces a challenging task in condensing the sections that differentiate between required and addressable implementation specifications, and we appreciate the intent behind streamlining these provisions. However, we are concerned about the flexibility of setting blanket standards for all regulated entities. Our member hospitals consistently promote safe data practices and collaborate with vendors nationwide to maintain patient trust in their ability to protect sensitive information. Despite this commitment, **we have reservations regarding the broad language used in certain provisions, which may limit the adaptability of the framework in addressing the diverse operational realities of health care entities.**

In particular, in 45 CFR 164.306(b), the proposed revision references the "effectiveness" of a security measure. We seek clarity on who is responsible for defining this effectiveness. In the event of a breach or cybersecurity incident, it remains unclear whether the original definition will continue to apply or if the agency will have discretion to redefine effectiveness post-incident. Similarly, in 45 CFR 164.306(c), while a minimum standard is proposed for regulated entities, the rule change does not specify what these minimum standards entail. **We strongly recommend that the agency provide more concise language regarding these minimum standards and explicitly consider differences in entity size, financial stability, and geographic location when setting these benchmarks.**

Finally, we are particularly concerned about the impact these broad, high-bar cybersecurity standards may have on hospitals in rural areas. Many rural hospitals already face significant challenges, including limited financial resources, staffing constraints, and potential impacts on access to care. If the cybersecurity bar is set too high without sufficient flexibility or accommodation for these factors, it could force these institutions to prioritize cybersecurity compliance over delivering essential health care services. **We urge DHHS to weigh these issues carefully and work collaboratively with stakeholders to ensure that the final rule supports robust security practices without inadvertently compromising patient care.**

Administrative Safeguards and Business Associate Arrangements:

Third-party vendors play an important role in modern health care by supporting the vast array of technologies and systems essential for running hospitals and health care systems. These partnerships ensure the secure handling of electronic protected health information (ePHI) and enable continual access to health care services and patient information. Although business associates are contractually obligated to provide these services, most regulated entities do not directly manage them. This distinction raises concerns regarding the vague requirement to monitor "when environmental or operational changes occur." Given the ever-evolving nature of software and technology, it is unclear whether these changes refer solely to adjustments within the regulated entity, changes at the business associate level, or both. If operational changes occur at the business associate, regulated entities may not be promptly informed about the severity or timing of these updates – potentially undermining their ability to manage risk effectively.

We also express concerns regarding the requirement that critical electronic information systems be restored within 72 hours following a service disruption. While hospitals strive to restore operations as quickly as possible, unforeseen circumstances, such as a cyberattack, can result in prolonged downtime. For instance, the cyberattack on ChangeHealthcare resulted in the critical billing system used by regulated entities being offline for several days, and in some cases, weeks. This experience underscores the need for clearer definitions of what constitutes a "critical system," whether it pertains to patient care, financial services, electronic health records, or other vital

functions. **Moreover, additional guidance is needed to help regulated entities assess the practical timelines for restoration based on the specific risks and operational realities they face.**

Finally, we appreciate the proposed requirement for business associates to report the activation of contingency plans within 24 hours, as it reinforces accountability and timely communication. However, we recommend that DHHS clarify that such notifications must be directed to a designated point of contact within the contracted entity and be required to confirm receipt rather than being issued as a public statement that could easily be overlooked. This measure would further ensure that critical information is communicated promptly and reliably. **Given that a significant number of the 10 largest health care data breaches have occurred among business associates (5) and health plans (4) – with hospitals often held accountable for these breaches – we urge DHHS to continue exploring mechanisms that hold business associates accountable.** Enhanced accountability is essential to protect ePHI and maintain the trust that patients place in our health care system.

Technical Safeguards, System Management, and Documentation:

Health systems rely on a vast network of connections, applications, and software to manage patient care, which includes numerous business associate agreements, data dictionaries, database schemas, and a wide range of software documentation. Managing this extensive and ever-evolving documentation is already complex, especially given the limited IT resources available to many health care systems. In the proposed rule, DHHS seeks to transition from an attestation- and policy-based approach to one that requires dedicated, detailed documentation of policies and procedures for safeguarding ePHI. This shift, as reflected in DHHS's own cost estimates, is expected to be both resource-intensive and costly, diverting staff from their core responsibilities of protecting ePHI.

Furthermore, the agency has not clearly delineated the extent of documentation required for both regulated entities and their business associates. Cybersecurity policies inherently involve actions by both parties, yet the proposed rule appears to impose new documentation burdens on regulated entities for processes traditionally managed by business associates. This could not only drive up compliance costs beyond current projections but also complicate coordination between health care organizations and their vendors. **We caution DHHS against moving too aggressively toward mandated dedicated documentation over existing attestation and general policy frameworks, as such an approach could inadvertently strain already limited resources and hinder effective cybersecurity management across the health care sector.**

Moreover, **we urge the Department to clarify the extent of the consistency and standardization of documentation across regulated entities.** It remains unclear whether DHHS will provide specific guidelines to ensure that the required documentation captures sufficient detail and what penalties, if any, will apply should these documents not be updated as mandated. Although the proposed rules discuss an annual update cycle (every 12 months), it is uncertain if this schedule applies to the newly mandated documentation in addition to updates triggered by critical operational or environmental changes. We seek additional clarity on the update schedule for these documents, including the flexibility to update them outside the scheduled window and the criteria that would justify such updates. Furthermore, it is not specified whether these plans are to be proactively transmitted to DHHS or made available upon request. If transmission is required, we are concerned about DHHS's internal ability to safeguard this sensitive cybersecurity information in light of its own previous data breaches.

Transition Provisions for Contracts and Plan Documents:

We appreciate the acknowledgment of the need for delayed adherence to the proposed rules regarding business associate agreements. Recognizing that these contracts may take time, and in some cases years, to fully comply with the proposed changes, we understand the challenges regulated entities face in adopting new security practices. In light of these challenges, we respectfully request that DHHS include a provision requiring regulated

entities to make a best effort to adopt the changes within the 12-month period. Alternatively, if compliance within this timeframe is not possible, entities should be allowed to document, with justification, the specific reasons for their inability to adopt the proposed rules.

Furthermore, as highlighted in our previous discussion on documentation requirements, AHA is concerned that a 12-month period is insufficient to develop technology- and system-specific documentation for the vast array of systems deployed in health care organizations, particularly for Critical Access Hospitals and multi-system hospitals. **We believe this process should be implemented over multiple years, accompanied by more direct guidance from DHHS, to avoid noncompliance and variations in documentation practices. At a minimum, if the final rule adopts these requirements, the process should be phased by different types of technology to ensure a manageable and realistic transition for all regulated entities.**

Request for Information – Emerging Technologies

Quantum Computing

Positive Impacts of Quantum Computing on Health care

Quantum computing promises to revolutionize health care by accelerating medical research and enhancing drug discovery. With its ability to process complex datasets at unprecedented speeds, quantum computing could significantly reduce the time required to identify correlations between genetic markers, environmental factors, and patient health outcomes. This enhanced computational power may lead to the development of more accurate diagnostic tools and personalized treatment protocols, thereby optimizing clinical decision-making. Additionally, quantum computing can enable advanced data analysis, which would not only streamline epidemiological studies and public health research but also support real-time processing of patient data to improve care delivery and operational efficiency.

Potential Negative Impacts and Concerns

We are particularly concerned about the widespread adoption of quantum computing by malicious actors. Such actors could leverage this technology to break through existing encryption algorithms, jeopardizing the security of sensitive patient information and disrupting critical health care systems. Moreover, there is a significant risk of unequal adoption across the health care industry. Facilities that cannot or do not adopt quantum-resistant technologies could become vulnerable, creating a gap that exposes these organizations to cyber threats while others advance. This raises an important question: how will the exact financial strains of adopting quantum computing balance against the expected efficiencies? While quantum computing might reduce the burden on staff and facilitate complex analyses, the direct costs of implementation and the ongoing expenses associated with managing and operating these systems remain unclear, compounding the challenges of widespread adoption.

Recommendations for Mitigating Quantum Computing Risks

We caution DHHS on the blanket adoption of quantum-resistant cryptography protocols for all regulatory entities at this stage. Given that the use cases for quantum computing in health care are still emerging and not yet widespread, there is much to learn about its full impact. **We recommend that DHHS continue to fund research into quantum computing and establish guardrails on the technology side rather than imposing premature regulations on health care institutions.** This approach would allow the industry to naturally adapt while ensuring that any regulatory changes are flexible enough to accommodate future innovations without inadvertently ostracizing entities or reducing patient access to care.

Artificial Intelligence (AI)

Positive Impacts of Artificial Intelligence on Health care

Artificial intelligence is now deeply integrated into health care, with applications ranging from advanced radiographic diagnostic tools that enhance early disease detection and treatment planning to various other innovations that streamline operations and reduce the workforce burden. For example, AI-driven image analysis has significantly improved the accuracy and speed of interpreting radiographs, while its predictive capabilities have the potential to revolutionize patient outcomes. Although there have been instances where AI is controversially employed – such as by some health insurance companies to make coverage determinations – **the overall promise of AI lies in its ability to drive efficiency, improve clinical outcomes, and unlock innovative solutions that we have yet to explore.**

Negative Impacts and Concerns

Despite its promising potential, AI also presents notable challenges. **We are particularly concerned about the widespread use of AI by health insurers to make decisions without human oversight, leading to instances where services may be denied without a physician’s review.** Furthermore, the increasing reliance on public AI tools to process sensitive health care data raises significant security and privacy concerns. An overreliance on AI in lieu of human judgment could compromise the nuanced decision-making required in complex clinical scenarios, potentially affecting the quality of patient care. **Moreover, the uneven adoption of AI technologies could widen the gap between well-resourced institutions and those that lack the means to implement such systems, further exacerbating disparities in health care delivery.**

Policy Recommendations for AI in Health care

Given the transformative potential of AI in health care, we recommend that DHHS continue to support its integration while addressing the associated risks. Increased funding for education and training on AI applications is essential, as is the adoption of minimum policies to ensure that patient data remains secure when these tools are utilized. We are proud of our member hospitals and their proactive internal policies that safeguard patient data and promote secure AI adoption. Additionally, on the health plan side, greater transparency is needed regarding the use of AI in coverage determinations, with clear safeguards to prevent inequitable denial of services. **With the right support from DHHS, AI can drive health care into a more efficient and innovative future without compromising patient privacy or the security of ePHI..**

Virtual and Augmented Reality (VR and AR)

Virtual and augmented reality have demonstrated remarkable use cases in health care, particularly in physician training. These tools enable medical students and practitioners to engage in immersive simulations that were previously unimaginable, ranging from practicing complex surgeries to navigating challenging clinical scenarios. By leveraging VR and AR, training programs can reduce costs and offer innovative, hands-on experiences that enhance clinical skills and decision-making.

We recognize that patient information is often used to generate the models and simulate unique patient conditions for training purposes. Consequently, it is imperative that clear standards be established to restrict the use of identifiable patient information by business associates providing these tools. Such safeguards will ensure that while the technology advances medical education, patient privacy is rigorously protected.

It is also important to note that academic hospitals are not the sole adopters of VR and AR technologies. Many hospitals have proactively integrated these tools into their staff onboarding processes and have utilized them to simulate emergency preparedness and cybersecurity scenarios. Given the broad potential benefits of these technologies, **we recommend that DHHS take active steps to enhance the availability of VR and AR tools for hospitals.** This should include dedicated funding for training resources that leverage these immersive technologies, ensuring that health care providers nationwide can harness their full potential while maintaining stringent privacy and security standards.

Conclusion:

In conclusion, the AHA recognizes the importance of modernizing the HIPAA Security Rule to enhance the protection of ePHI while maintaining the integrity of health care operations. Our member hospitals remain committed to cybersecurity, data privacy, and patient trust. **While we understand the intent of the previous administration and the impact of recent cybersecurity events, we urge the new administration at DHHS to approach these regulatory changes with a balanced and practical framework that considers the financial, operational, and technological challenges facing health care entities – particularly those in rural areas.**

To ensure the successful implementation of the proposed updates, we recommend a phased approach that allows hospitals adequate time to adapt to new security measures without jeopardizing patient care. Furthermore, we emphasize the need for clear definitions, flexibility in compliance standards, and stronger accountability mechanisms for business associates, given their critical role in safeguarding ePHI.

As health care continues to evolve with emerging technologies, it is essential that regulatory frameworks remain adaptable, enabling hospitals to provide high-quality care while ensuring robust cybersecurity protections. We appreciate the opportunity to provide feedback and look forward to continued collaboration with DHHS to develop policies that promote both security and sustainability in health care.

Thank you, again, for the opportunity to comment on 45 CFR Parts 160 and 164: HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information. Please let me know how I can provide further information to help you as you move forward.

Sincerely,

A handwritten signature in black ink that reads "Bo Ryall". The signature is fluid and cursive, with the first name "Bo" being larger and more prominent than the last name "Ryall".

Bo Ryall
President & CEO
Arkansas Hospital Association
boryall@arkhospitals.org