National Rural Health Association

March 7, 2025

Secretary Robert F. Kennedy Jr.
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

RE: RIN 0945-AA22; Comments on HIPAA Security Rule Proposed Modifications to establish national standards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). Health plans, health care clearinghouses, and any health care providers that transmit information electronically ("regulated entities") are subject to the Security Rule and any proposed updates.

Submitted electronically via regulations.gov.

Dear Secretary Kennedy,

The National Rural Health Association (NRHA) appreciates the opportunity to comment on the Department of Health and Human Services' (HHS) proposed modifications to the HIPAA Security Rule as published in the Federal Register on January 6, 2025. While we acknowledge the intent to strengthen cybersecurity protections for electronic protected health information (ePHI), we must emphasize that the proposed rule presents insurmountable challenges for rural health care providers.

NRHA is a non-profit membership organization with more than 21,000 members nationwide that provides leadership on rural health issues. Our members include rural community hospitals, critical access hospitals, long-term care providers, doctors, nurses, and patients. We work to improve rural America's health needs through government advocacy, communications, education, and research.

HHS, through its Office for Civil Rights (OCR), has issued a proposed rule to modify the HIPAA Security Rule to strengthen cybersecurity protections and clarify compliance requirements. These updates aim to address the exponential rise in cyberattacks in the health care sector, which saw over 54 million patients affected by data breaches in 2022 alone. According to the HHS Cybersecurity Program, 60% of the ransomware attacks in 2020 were aimed at healthcare organizations.

Unfortunately, small rural hospitals are more susceptible to cyberattacks than larger hospitals.[1] HHS recognizes that small rural providers are more likely to rely on older technology and face more difficulties recruiting security professionals. This is because rural hospitals do not have the resources or capital to upgrade to more modern technology that can help protect them from cyberattacks. Similarly, rural hospitals do not have the infrastructure or bandwidth to comply with stringent, inflexible federal requirements around cybersecurity. Instead of unfunded mandates, rural providers need resources to help them achieve cybersecurity preparedness.

[1] https://www.ruralhealthinfo.org/rural-monitor/cybersecurity-attacks and https://www.ruralhealth.us/getmedia/ad0774a2-49b4-4f9a-b2c5-2edf0eaf6bcf/2024-NRHA-Cybersecurity-Rural-Health-policy-brief.pdf

RuralHealth.US
50 F. St., N.W., Suite 520
Washington, DC 20001 | 202-639-0550

Overall, NRHA is disappointed with the lack of consideration for rural providers in the proposed rule. NRHA cannot support the rule as written without inclusion of flexibility in the aggressive proposed timelines, federal support for rural providers to implement the proposed changes, or exemptions for rural providers.

Overview of Key Proposed Changes and Challenges for Rural Providers

1. **Elimination of Implementation Flexibility**: **Excessive Compliance Costs.** The mandated investments—including multi-factor authentication, encryption, network mapping, technology asset inventories, penetration testing, and vulnerability scanning—are cost-prohibitive without additional resources for small and rural health care facilities that already operate on narrow, if not negative, financial margins.
2. **Overly Broad and Incomplete Language**: The proposed rule contains ambiguous definitions and vague requirements, such as "relevant electronic information systems," "resiliency," and "critical risk." Further clarification is needed to avoid confusion and inconsistent adherence, placing additional burdens on rural providers.
3. **Workforce Security Requirements**: The NPRM proposes modifications requiring written policies to ensure proper workforce access to ePHI. While security awareness training may be beneficial, extensive documentation and compliance audits will be cumbersome for rural facilities with limited personnel.
4. **Mandatory Encryption and MFA Requirements**: While these measures can enhance security, they pose significant financial and operational barriers to rural providers who may lack the necessary technical support.
5. **Increased Documentation Burden**: The requirement for continuous documentation, technology asset inventories, and annual compliance audits will stretch rural health care resources thin without meaningfully reducing cybersecurity risks.
6. **Short Compliance Timelines**: The proposal mandates a 180-day compliance period following the effective date, which is an insufficient time period for small and rural providers to implement the necessary operational and technological changes. Delays of implementation are needed to allow small and rural providers to be able to come into compliance with any new requirements.

HHS acknowledges that rural providers are high-risk targets for cyber threats but asserts that they can determine the security measures most reasonable and appropriate for their operations. However, the proposed rule does not offer resources, exemptions, or tailored compliance pathways for rural providers, despite requesting comments on whether it sufficiently accounts for their needs and capabilities.

NRHA Recommendations:

NRHA fully supports strengthening cybersecurity protections but urges HHS to implement a more balanced approach that enhances security without endangering the financial viability and service capacity of rural health care providers. Specifically, NRHA recommends:

RuralHealth.US
50 F. St., N.W., Suite 520
Washington, DC 20001 | 202-639-0550

- Retaining the flexibility of "addressable" implementation specifications for rural providers so that they may adopt appropriate security measures based on their existing resources.
- Clarifying key regulatory definitions to minimize regulatory confusion.
- Providing financial assistance, grants, or targeted technical support to aid rural providers in compliance efforts.
- Extending the compliance timeline to at least three years for rural providers to allow for phased implementation.
- Balancing documentation requirements with meaningful security improvements to ensure compliance efforts focus on practical risk mitigation rather than administrative burdens.

C. Section 164.306—Security Standards: General Rules

The notice of proposed rulemaking (NPRM) eliminates the flexibility of "addressable" implementation specifications, instead making all specifications mandatory. The current implementation specifications were designed to permit flexibility for regulated entities when determining their compliance meaning small, rural providers are able tailor their limited resources and consider the overall cost when designing their plan to comply. HHS is proposing to require all providers to encrypt electronic personal health information (ePHI) and deploy multi-factor authentication for all technology assets, among other provisions. While this may enhance security in larger, well-resourced institutions, it removes necessary flexibility for rural providers with limited cybersecurity infrastructure. The proposed changes do not consider the resource constraints of rural providers, who often lack the IT infrastructure to implement these standards uniformly. NRHA urges HHS to retain flexibility to allow providers to tailor security measures to their operational standards.

D. Section 164.308—Administrative Safeguards.

The NPRM mandates written policies to ensure appropriate workforce access to ePHI while restricting unauthorized access. While NRHA supports security awareness training, the additional documentation and compliance burdens will be overwhelming for rural providers with limited staff. HHS should consider a phased implementation plan for rural providers.

The rule introduces enhanced risk analysis mandates, including asset inventories and network mapping. These requirements are resource-intensive and difficult for small, rural health care providers to achieve without additional technical assistance and resources.

Last, HHS proposes that entities establish security incident response plans and restore electronic systems within 72 hours of a breach. Many rural providers lack a dedicated IT team or personnel that could feasibly meet this requirement. As such, NRHA recommends a longer timeframe for rural providers.

E. Section 164.310—Physical Safeguards

The NPRM requires regulated entities to establish stringent physical security controls for electronic systems. Many rural providers operate in aging facilities with limited funding for infrastructure upgrades. High inflation and rising interest rates make it harder for aging facilities to qualify for loans

RuralHealth.US
50 F. St., N.W., Suite 520
Washington, DC 20001 | 202-639-0550

or other financed upgrades to their facilities to meet the ever-changing standards of medical care.[2] Further, ever increasing operating costs amid lower payments from insurance plans makes it harder for small hospitals to fund large capital improvement projects.[3]

F. Section 164.312—Technical Safeguards

HHS proposes mandatory encryption of ePHI and multi-factor authentication (MFA) whenever personnel are seeking to access ePHI. While these measures improve security, they are prohibitively expensive and complex for rural health infrastructure. In many circumstances, the mandatory technical safeguards would mean massive changes to their electronic information systems and without additional resources, rural hospitals would not realistically be able to comply. NRHA acknowledges that HHS creates some flexibility for regulated entities that use technology that does not support MFA and would provide the entity a "reasonable and appropriate" period of time to migrate ePHI to technology that does support MFA. However, NRHA requests further flexibility in compliance timelines and additional funding and technical assistance opportunities.

NRHA thanks HHS for the opportunity to provide comments on this proposed rule. We look forward to continuing our work together to ensure safe access to quality care for rural beneficiaries. If you have any questions, please contact NRHA's Government Affairs & Policy Director, Alexa McKinley Abel, at amckinley@ruralhealth.us.

Sincerely,

Alan Morgan
Chief Executive Officer
National Rural Health Association

[2] https://www.fiercehealthcare.com/providers/rural-hospitals-are-caught-aging-infrastructure-conundrum#:~:text=Rural%20hospitals%20throughout%20the%20nation,changing%20standards%20of%20medical%20care.
[3] https://www.fiercehealthcare.com/providers/rural-hospitals-are-caught-aging-infrastructure-conundrum#:~:text=Rural%20hospitals%20throughout%20the%20nation,changing%20standards%20of%20medical%20care.

RuralHealth.US
50 F. St., N.W., Suite 520
Washington, DC 20001 | 202-639-0550