Submitted Electronically

March 7, 2025

Anthony Archeval
Acting Director
U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
200 Independence Avenue SW
Washington, DC 20201

Re: HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information (RIN Number 0945-AA22)

Dear Acting Director Archeval,

On behalf of our more than 5,400 nonprofit and mission-driven aging services providers, LeadingAge is pleased to offer the following comments in response to the Office for Civil Rights (OCR) HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Health Information proposed rule. Our members serve older adults across the country and along a full spectrum of services and supports, such as senior housing including affordable housing, assisted living and memory care, skilled nursing, home health, and hospice, and life plan communities that offer a continuum of housing and services to their residents.

We appreciate and support the goal of strengthening data security and protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI). However, we write to express our concerns regarding the feasibility of implementing the proposed rule and the impact it would have on aging services providers, including significant burdens on staff and budgets.

For the reasons set forth below, we believe significant changes are needed to the rule as proposed.

I. The Proposed Rule Pursues Important Goals But Imposes Excessive Administrative Burden and Cost

Aging services providers understand the importance of securing ePHI appropriately and work to ensure that their systems deliver proper protection. The volume and complexity of the OCR's proposals, however, would significantly increase compliance requirements, including mandatory annual risk analyses, employee security training, enhanced system logging, and stricter audit controls, to name only a few of the many new requirements.

While we support robust security measures, these requirements would place a heavy administrative and financial strain on aging services providers. In part, this is because aging services providers did not receive federal *HITECH* incentives for the adoption of health information technology (IT). As a result, they have less digitally-mature systems than hospitals and other providers that did receive incentives, and they will have significantly farther to go to achieve compliance with the proposed requirements.

Even more importantly, this is because the rule would apply the standards and specifications equally to all HIPAA covered entities, from small providers to the largest of health systems, and to health plans and clearinghouses.

The proposed rule acknowledges, for example, that small and rural health care providers may have needs and capabilities that differ from those of other regulated entities: "For example, small health care providers and rural health care providers are often located at a greater distance from other health care providers. It may be more challenging for them to attract and retain clinicians and administrative support staff. They also face difficulty attracting and retaining security experts and must make difficult decisions regarding investments in competing priorities."[1] Yet OCR concludes, all things considered, that "small and rural health care providers have both the need to comply with the proposals in this NPRM and the capability of doing so."[2]

The reality is that not all regulated entities are similarly situated, and OCR should not seek to regulate them all in the same way. Breaches of the ePHI held by some organizations pose significantly higher risk for industry disruption than others, and some regulated entities have significantly greater capacity than others to meet the proposed standards. Relating to the second point, the American Health Information Management Association succinctly observes as follows in its comment letter submitted to this docket on February 27:

> *Throughout the proposed rule, OCR hypothesizes many HIPAA-covered entities do not follow the requirements within the HIPAA Security Rule because they choose not to or do not understand the rule. In reality, those unable to attain compliance often fail to do so due to a lack of resources available or work to achieve compliance to the best of their knowledge but may require additional clarity on the current requirements.*
>
> *The HIPAA Security Rule requirements are critical to ensuring the security of an entity and its ePHI, however, these requirements are not funded and the lack of flexibility in the number of compliance pathways poses barriers to compliance. Without resources and assistance, entities often have no choice but to prioritize the requirements they are financially able to implement.* [3]

This holds true for aging services providers, which vary in terms of their current integration of IT infrastructure and cybersecurity measures, the degree to which they have internal, dedicated staff with the expertise needed to do this work, and the financial resources available to address these matters.

The proposed rule would place a significant administrative strain on existing staffing, even for organizations with strong IT support systems already in place. New obligations, such as enhanced logging, auditing and access control, continuous monitoring, rapid access revocation, and stricter authentication processes would create a considerable workload for IT and compliance staff.

Meeting the proposed standards would impose significant financial burdens as well as administrative ones. For providers that have little or lean internal IT expertise, this would mean increased expenditure on external supports. And some LeadingAge member organizations that do have internal IT expertise noted that compliance would require them to one or two new cybersecurity personnel. Of course, investments in technology upgrades would be required in many cases, as well, the cost of which will itself also reflect implementation of the proposed standards.

---

[1] HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, 90 FR 898 (proposed Jan. 6, 2025) at 90 FR 918.

[2] 90 FR 919

[3] Comment from American Health Information Management Association (AHIMA), HHS-OCR-2024-0020, HHS-OCR-2024-0020-0001, 2024-30983

OCR Significantly Underestimates the Costs of Implementation

We reiterate the commitment of aging services providers to the underlying goals of the proposed rule, but we must comment further on the financial implications. The proposal's Regulatory Impact Analysis (RIA) states, in part, that if adopted, it "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."[4]

We believe the actual costs would be significantly higher.

Our colleagues and LeadingAge Illinois and Iowa noted in their comment letter[5] that many nursing homes may need to engage consultants to assess what would be needed to achieve compliance. They note that an IT contractor that works with many long-term care providers estimated a cost of $10,000-$30,000 for such an evaluation, which may vary depending on the nature of existing systems in place for a given facility. If even half of the 14,785 active nursing home providers would need to complete a technology evaluation to prepare for a final rule, they calculate, it would cost a minimum of $73.9 million dollars, not including equipment and services that would be necessary to achieve compliance.

In addition to that helpful insight, we believe the estimates of other specific costs set forth in the RIA are significantly understated, both in terms of the hours of work OCR estimates would be invested in certain activities and of the estimated cost for that work to be done.

- OCR estimates it would take 2 hours by an information systems analyst to conduct a security rule compliance audit.[6] The LeadingAge Illinois/Iowa letter suggests it would take much longer with related costs.
- Network segmentation is a complex and lengthy, interdisciplinary process. Yet OCR estimates 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.[7]
- OCR estimates 3 hours for penetration testing.[8] In the experience of one LeadingAge member, penetration tests have typically been greater than 40 hours.
- OCR estimates that, on average, the portion of business associate agreement revisions that results from the rule's modifications would take one hour of a lawyer's time for each regulated entity, and indicates that a lawyer's fully loaded hourly wage is $169.68.[9] Both the time needed and the assumed hourly rate are vastly understated.[10]

For many of our nonprofit and mission driven member organizations, which rely heavily on Medicaid and Medicare reimbursement that is insufficient to cover the full costs of delivering services, full implementation of the proposed requirements may not be feasible, and certainly not within the proposed implementation timeline.

---

[4] 90 FR 992

[5] Comment from LeadingAge Illinois/Iowa, HHS-OCR-2024-0020, HHS-OCR-2024-0020-0001, 2024-30983

[6] 90 FR 997

[7] 90 FR 998

[8] 90 FR 999

[9] 90 FR 1000

[10] A U.S. News & World Report article, for example, notes that attorneys charged a national average of $327 per hour in August 2023. See https://law.usnews.com/law-firms/advice/articles/what-does-hiring-a-lawyer-cost.

Cost burdens are especially important for OCR to consider in light of President Trump's January 31 Executive Order, Unleashing Prosperity Through Deregulation, stating that the Administration's policy is "to significantly reduce the private expenditures required to comply with Federal regulations."[11]

We believe OCR should revise and republish the proposed regulatory impact analysis to address its shortcomings before this rule is finalized.

II. Comments on Specific Standards and Implementation Specifications

In this section we offer comments on selected safeguards included in the proposed rule. These are only some of the many issues that will arise if the proposal is finalized, which are addressed well by other stakeholders that have submitted letters.

A. Administrative Safeguards

Section 164.308(a)(1)(i-ii)—Standard: Technology Asset Inventory

This standard and OCR's new implementation specifications would require an inventory of all technology assets and a network map that illustrates the movement of the regulated entity's ePHI through its electronic information systems. In addition to creating the initial inventory and map, entities would be required to update this work product on an ongoing basis but at least every 12 months, and whenever there is a change in the entity's environment or operations that may affect ePHI, including but not limited to the adoption of new technology assets; the upgrading, updating, or patching of technology assets; newly recognized threats to the confidentiality, integrity, or availability of electronic protected health information; a sale, transfer, merger, or consolidation of all or part of the covered entity or business associate with another person. This proposal creates very complex administrative requirements and is a significant departure from current standards.

While we understand the value of creating and maintaining an accurate, real-time inventory and network map, doing so, and especially keeping them current in accordance with the proposed maintenance requirements, is complex and challenging work and will be burdensome to implement, particularly for smaller entities with fewer resources.

Among other challenges, our members have shared that no widely available tool exists to track real-time ePHI movement across an entire network. Some senior living providers already use dynamic network mapping tools, but tracking ePHI movement in real time would require significant software investment and ongoing monitoring, adding to compliance costs. Further, it appears this requirement may be overly broad, potentially including non-clinical systems that interact with an electronic health record (EHR), further complicating compliance.

If these implementation specifications were addressable instead of required, regulated entities would have greater flexibility to conduct, maintain, and update their asset inventory and network map in a manner appropriate for their organization.

[11] Executive Order 14192 of January 31, 2025 (90 FR 9065); see also Fact Sheet: President Donald J. Trump Launches Massive 10-to-1 Deregulation Initiative (Jan. 31, 2025)

Section 164.308(a)(4)(i-ii)—Standard: Patch Management

This section[12] introduces requirements for creating patch management policies and procedures, reviewing, testing and modifying (if needed) such policies and procedures at least every 12 months. An additional specification would require patching within 15 days to address a critical risk and within 30 days to address high risks, with limited exceptions.

Frequent patching and system updates required under the proposed rule could lead to increased system downtime, directly affecting resident services. Any interruptions in EHR access or communication systems could have serious consequences for senior residents, who depend on timely and accurate care coordination. We also note that many aging services providers rely upon older, legacy systems that are not easily patched.

§ 164.308(a)(6)(i) Standard: Sanction Policy

This standard would require regulated entities to apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the regulated entity. While the term "appropriate sanctions" is not defined, we are concerned that, if implemented, the proposed standard would potentially force providers to terminate employees who fail to meet cybersecurity standards, perhaps even when an event of noncompliance is inadvertent or a case of human error, rather than a reckless or intentional act. With ongoing workforce shortages, this requirement could further strain staffing levels. We encourage OCR to provide guidance on enforcing compliance without exacerbating workforce challenges.

Section 164.308(a)(9)(i)—Standard: Workforce Security

In general, this standard requires regulated entities to implement written policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information and relevant electronic information systems, and to prevent those workforce members who are not authorized to have access from obtaining access to electronic protected health information and relevant electronic information systems.

Among the proposed implementation specifications is one that would require regulated entities to terminate access to electronic health records as soon as possible, but not later than one hour after the workforce member's employment or other arrangement ends.

We believe this proposed requirement is stricter than other existing requirements, goes beyond industry standards, and will require significant change in how access is provided and terminated within organizations, especially for organizations that provide services 24 hours per day, 7 days per week, as many aging services providers do.

We recommend that OCR provide for a longer period of time – for example: as soon as possible and not later than the close-of-business on the next business day.

[12] See also the technical safeguard at section 164.12(h)(2)(iv).

§ 164.308(a)(10)(e) Standard: Information Access Management

This proposed standard includes a network segmentation specification requiring regulated entities to establish and implement written policies and procedures that ensure that a covered entity's or business associate's relevant electronic information systems are segmented to limit access to electronic protected health information to authorized workstations.

Segmentation of electronic health information systems is a valuable practice to safeguard against the cascading impacts of cyber threats and attacks. However, this proposal is complex and will be burdensome to implement, especially for smaller entities. We refer again to the American Health Information Management Association comment letter, which states:

> *Network segmentation requires entities to develop contracts with new vendors and implement new systems, which will involve data migration, and is a lengthy and intensive process. Additionally, having data and assets on separate networks presents challenges in getting devices on those segments to communicate. …. There is also a lack of clarity about what constitutes reasonable and appropriate network segmentation as written in the rule. Reasonable and appropriate segmentation will vary depending on the entity's size and characteristics, business associate agreements, the entity's level and volume of health and administrative data, the number of patients the entity serves, how complex the risk analysis is, as well as additional factors that impact an entity's ePHI.*[13]

If finalized, OCR should provide a lengthy implementation timeline, as addressed below, and provide decision-making tools, as well as technical support and guidance to clarify the level of segmentation needed and how segmentation would be impacted by an entity's characteristics.

§ 164.308(a)(12): Incident Response

The proposed rule requires the creation of an incident response plan, the testing of such plan at least annually, and the identification, remediation, mitigation, eradication and documentation of both known and ***suspected*** security incidents.

We appreciate the importance of planning for and reacting to security incidents, but we believe the requirement to identify, respond to, mitigate, remediate, eradicate, and document suspected incidents will likely be a significant shift for many organizations, requiring additional documentation and processes.

While regulated entities can and do learn from suspected incidents, we question the need to extend the full range of requirements established under this section to such incidents. Further, from a drafting standpoint, a suspected incident should not trigger a need to "remediate" or "eradicate," since there would be nothing to remediate or eradicate unless it turned into an actual incident.

B. Technical Safeguards

Section § 164.312(f): Standard: Authentication

Within this standard requiring technical controls to verify that a person or technology asset seeking access to electronic protected health information is the one claimed, OCR proposes to require the use of multi-

[13] See footnote 3.

factor authentication, meaning authentication of the user's identity through information known by the user, an item possessed by the user, and a personal characteristic of the user. A user would be required to provide at least two separate factors from two separate categories to authenticate identity.

It is important to note that aging services providers may not be in a position to control all factors affecting compliance with this proposed requirement. For example, many aging services providers rely on software that does not currently support multi-factor authentication or advanced encryption. This is another example where OCR should allow for flexibility, including a longer implementation timeline than is currently proposed.

In this context, our members have also raised questions concerning interplay with the proposed rule's new definition (§ 164.304) of "electronic information system," a term that is incorporated into various implementation specifications. As other commenters have noted, the new requirements in the proposed rule apply both to electronic information systems that create, receive, maintain, or transmit ePHI, but also to other systems that are connected to or otherwise affect electronic information systems that potentially affect ePHI.

Specifically, we are concerned that it may result in required multifactor authentication (or encryption, under a separate provision) with respect to non-traditional healthcare systems, such as senior living, where food service, gift shop, and property management systems may now fall under HIPAA compliance. In the dining area of a senior living community, for example, the system into which a staff member enters a resident's meal order may provide a notification concerning dietary recommendations or restrictions. We believe requiring access controls each time a staff member utilizes that system would be an unanticipated consequence and an unnecessary burden. Extension of the requirements to ancillary systems used in dining or gift shops would seem unnecessary, as the focus should be on primary systems that most often directly interact with ePHI.

§ 164.312(h): Standard: Vulnerability Scanning

This section of the proposed rule requires covered entities and business associates to conduct vulnerability scans at least every six months, monitor sources of known vulnerabilities on an ongoing basis, perform penetration tests at least once every 12 months, and install patches on a timely basis. These activities must be done against relevant electronic information systems. As referenced above, this will require a significant budget for the use of external penetration testers or, if feasible, the development of an internal capability to perform the tests.

C. Organizational Requirements

The proposal's expanded requirements for business associate compliance impose additional administrative and cost burdens. Verifying and ensuring compliance of all third-party vendors with access to ePHI, including software providers, billing services, and telehealth platforms, would require expertise and dedicated resources that many providers lack. Additionally, revising business associate agreements will be a complex and time-consuming process.

To reduce this burden, we recommend that OCR consider the time and expense burden placed on providers as part of these investigations and provide education to all regulated entities to ensure business associates are complying with the Security Rule, with the goal of lightening the burden on HIPAA covered entities.

III. The Proposed Implementation and Enforcement Timeline Is Unrealistically Short

OCR's proposal to require full compliance within 240 days after publication of a final rule is unreasonable. Even for aging services providers with relatively mature IT systems, it will not be feasible to absorb, understand and implement the deep and broad body of new requirements within this timeframe.

We call on OCR instead to establish a phased-in approach, over a much longer period, so that regulated entities have sufficient time to establish and implement policies, procedures, and practices to achieve compliance with new or modified standards*.* We recommend a phased and extended timeline of three to four years.

IV. Recommendations

If OCR moves forward with this proposal, we ask that the Department of Health and Human Services do the following:

- Conduct further engagement with the communities of regulated entities that the rule would impact, beyond this initial 60-day comment period, to build deeper understanding of feasibility, consider flexibilities for organizations with fewer resources and less mature systems, and prioritize the establishment of reasonably-burdensome requirements that will reduce risks in a meaningful way and not unduly impact workflows or reduce time spent in direct service to residents, clients and patients.
- Preserve the distinction between addressable and required implementation specifications to provide regulated entities with the flexibility they need to address their specific assessed risks and situation.
- Build in flexibility, allowing for alternative compliance paths, or exemptions for organizations with demonstrated security measures already in place, and a longer, more gradual implementation timeline that prioritizes requirements for the highest risk activities and gives regulated entities adequate time to prepare.
- Clarify definitions to prevent non-healthcare systems, such as senior housing, from being unnecessarily subject to HIPAA.
- Improve vendor accountability and provide clearer guidance on compliance expectations.
- Endorse and work to provide positive supports, such as federal funding (similar to Meaningful Use dollars in hospitals that incentivized the use of industry standards), to help aging services providers implement these changes. As OCR notes in the proposed rule, "[t]here are no Federal funds directed at Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance activities"[14] and, as noted above, financial incentives have not been legislatively extended to Medicare participating long-term and post-acute care providers (skilled nursing facilities, long-term care hospitals, inpatient rehabilitation facilities, home health agencies, and hospice programs) to acquire or upgrade health IT and implement interoperable electronic health record technology.
- Provide targeted support to help regulated entities meet the proposed requirements, through funding, expertise, and technical guidance to implement cybersecurity best practices. This will be especially critical for smaller and rural providers. Establishing the new standards and transitioning into an enforcement mode will simply not work.

[14] 90 FR 992

- Establish public-private partnerships (e.g., the U.S. Department of Homeland Security, National Institute of Standards and Technology) to develop reasonable, sector-specific cybersecurity standards.

Conclusion

The combination of the depth and breadth of the proposed requirements, without funding support and on an unreasonable timeline would impose significant burdens. While we support HIPAA's goal of strengthening security and protecting ePHI, we urge regulators to consider alternative compliance models that account for the unique operational and resource constraints of aging services providers.

LeadingAge appreciates the opportunity to share our perspective on the proposed rule, and we welcome the opportunity to engage with you further. Thank you for your consideration, and please contact me (jlips@leadingage.org) if we can answer any questions or provide additional information.

Sincerely,

Jonathan W. Lips

Vice President Legal Affairs

About LeadingAge*: We represent more than 5,400 nonprofit and mission-driven aging services providers and other organizations that touch millions of lives every day. Alongside our members and thirty-six partners in forty-one states, we use applied research, advocacy, education, and community-building to make America a better place to grow old. Our membership encompasses the continuum of services for people as they age, including those with disabilities. We bring together the most inventive minds in the field to lead and innovate solutions that support older adults wherever they call home.*