March 7, 2025

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

Secretary Robert F. Kennedy, Jr.
U.S. Department of Health & Human Services (HHS)
Office for Civil Rights (OCR)
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

RE: HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information Proposed Rule [RIN Number 0945-AA22]

Dear Secretary Kennedy,

On behalf of the Long Term & Post-Acute Care (LTPAC) Health IT Collaborative, we are pleased to provide written comments regarding *HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information Proposed Rule (RIN 0945-AA22)*. The LTPAC Health IT Collaborative, whose members include provider and professional associations and national experts in post-acute care settings, nursing homes, senior living communities, assisted living, home health care, physicians, nursing, pharmacists, rehabilitation, and healthcare information systems, appreciate the opportunity to share our expertise on the ability of the sector to meet the requirements in the proposed rule.

Bad cyber actors put our entire nation's healthcare system at serious risk, including the LTPAC sector. The cyber threats that LTPAC, behavioral health and other providers face are the same as those confronting acute and ambulatory care providers who operate within hospital systems or physician offices where *Health Information Technology for Economic & Clinical Health (HITECH) Act* funds have fostered health IT adoption rates nearing 100%. While the risks are the same, the resources to combat cyber threats are not. For example, hospitals hire Chief Information Officers (CIOs) to oversee health IT systems and networks staffed by health IT professionals. In contrast, health IT vendors serving the LTPAC sector often double as *de facto* technical support teams for their LTPAC provider clients, few of whom employ any IT staff.

The Collaborative understands the importance of enhanced cybersecurity protections to maintain the privacy and security of protected health information. We are concerned that the one-size-fits-all approach outlined in the proposed rule does not consider critical differences in care settings that must be addressed. We highlight some of our shared, high-level concerns and support the more detailed responses and recommendations submitted by Collaborative members.

Cost & Burden of Proposed Changes Fail to Consider Differences in Providers' Risk Profiles

Because LTPAC providers did not receive federal *HITECH* incentives for the adoption of health IT, the digital maturity of LTPAC settings lags behind hospitals and physician offices. The December 2023 study published by the HHS/ ASPE's Office of Behavioral Health, Disability and Aging Policy found that "LTPAC providers are adopting EHRs to support their clinical and business needs (80% for nursing homes and home health), but interoperable exchange of health information is not routine or widely used."[1]

One of the largest gaps in digital maturity relates to the exchange of health information across care settings. For providers who struggle to meet myriad federal regulations, this gap makes achieving compliance with the proposed changes and timelines nearly impossible, creating disproportionate administrative and financial burden. Moreover, we believe that the burden on LTPAC providers is excessive compared to the risk profile of these care settings. The LTPAC sector overall participates in limited health data exchange, which helps to limit the impact that a cyber breach by an LTPAC provider could have on other providers. This smaller scale impact pales in comparison to the risk that a cyber incident at a hospital would pose to the rest of the healthcare system. For example, in 2024, the massive cyber breach of Change Healthcare affected nearly one in three health records nationwide. No LTPAC organization could approach that level of impact on the healthcare system.

The Collaborative recommends that OCR scale compliance with the proposed changes to the HIPAA Security Rule according to the risk profile of the HIPAA regulated entities.

Reconsider Implementation Timeline based on Digital Maturity and Resources Needed

Most LTPAC providers are less digitally mature than providers in hospitals and physician practices that received HITECH funding and therefore starting behind in meeting the new

[1] https://aspe.hhs.gov/reports/hit-adoption-utilization-ltpac-settings

proposed cybersecurity requirement. We agree with the National Committee on Vital & Health Statistics (NCVHS) that security standards need to evolve to address changes in the healthcare environment, but implementation timelines need to accommodate varying levels of digital maturity. The proposed 180-day compliance deadline following the 60-day implementation period following the proposed final rule (240 total days), is not adequate for most LTPAC providers to meet the requirements of the rule given the extensive administrative processes required, workforce challenges, and limited resources.

We would like to see every LTPAC provider first using the ten essential Cybersecurity Performance Goals. For this reason and others, we encourage a phased approach to compliance. The implementation compliance timeline approach should not be an all-or-nothing short deadline but should instead include a phase-in approach extending over multiple years, targeting the highest cybersecurity risk areas first. The phase-in approach should include flexibilities that consider the current digital maturity and resource availability of the covered entities under a flexible continuous improvement model rather than as a rigid one-size-fits-all compliance floor model. The compliance floor model places excessive burdens on low risk profile providers while creating little incentive for high risk profile organizations to improve.

Recommendation: The Collaborative recommends that OCR extend the compliance timeline for LTPAC providers and implement a phased approach aligned with the organization's digital maturity focused on the 10 Essential Cybersecurity Performance Goals. We also recommend resources be made available to support LTPAC providers in meeting the requirements and set a deadline commensurate with resource availability.

Resources and Potential Solutions:

The Collaborative wholeheartedly supports a greater focus on cybersecurity practices across the healthcare system. We respectfully suggest that OCR reconsider how these proposals could be implemented effectively. There will be challenges for LTPAC providers with the implementation and operationalization of the requirements due to the administrative burden which will increase paperwork over patients.

We in the LTPAC sector are keenly aware of how limited resources are. We recommend that any shortfall in compliance with the *HIPAA Security Rule* not result in punitive measures for those sectors that did not receive *HITECH* incentives to modernize their health IT systems. Instead, HHS should direct resources and support to those providers to improve their ability to operate in accordance with cybersecurity protections proposed by OCR.

Recommendation: The Collaborative recommends the following resources and solutions:

- Provide federal funding (similar to HITECH Meaningful Use program stages for hospitals and physician practices) to help aging services providers implement these changes.
- Establish a cybersecurity risk profile scale for and within each healthcare sector listed in Table 4 of the proposed rule that would be subject to the ePHI cybersecurity provision policy updates. The requirements would be targeted and scaled to consider and reflect the unique operational differences between each sector. This includes considering the risk mitigation to burden ratio for specific provisions so that the required burden is scaled to the cybersecurity risk profile of the provider.
- Improve business associate accountability and provide clearer guidance on compliance expectations.
- Clarify definitions to prevent non-healthcare systems from being unnecessarily subject to HIPAA (e.g., gift shops, food service, property management systems)
- Establish public-private partnerships (e.g., Homeland Security, NIST) to develop reasonable, sector-specific cybersecurity standards.
- Offer support resources and outreach programs to help smaller providers comply with the requirements.

The LTPAC Health IT Collaborative welcomes the opportunity to discuss the challenges ahead and the ways that we can advance the necessary changes to improve care while addressing costs and provider burden. If you or your staff would like to discuss in further detail, please contact Michelle Dougherty at mvldougherty@gmail.com as she is the facilitator of our Collaborative.

Sincerely,

The LTPAC Health IT Collaborative

For a list of LTPAC Health IT Collaborative members, please visit us at www.LTPACHIT.org.