National Alliance for Care at Home

March 7, 2025

Anthony Archeval, Acting Director
Office for Civil Rights
U.S. Department of Health and Human Services
Attention: HIPAA Security Rule NPRM
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue SW
Washington, DC 20201

RE: **Docket No. HHS–OCR–0945–AA22**, HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Dear Acting Director Archeval:

The National Alliance for Care at Home (Alliance) appreciates the opportunity comment on the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information proposed rule. The Alliance is the unified voice for providers delivering high-quality, person-centered healthcare to individuals, wherever they call home. Our members are providers of different sizes and types—from small rural agencies to large national companies—including government-based providers, nonprofit organizations, system-based entities, and public corporations. Our members, including over 1,500 providers representing 10,000 offices and locations, serve over 4 million patients nationwide through a dedicated workforce of over 1 million employees, staff, and volunteers. Formed through the joint affiliation of the National Association for Home Care & Hospice (NAHC) and the National Hospice and Palliative Care Organization (NHPCO), the Alliance is dedicated to advancing policies that support care in the home for millions of Americans at all stages of life, individuals with disabilities, persons with both chronic and serious illnesses as well as dying Americans who depend on those supports.

Our member providers—including home health agencies, hospices, palliative care practitioners and organizations, and personal care agencies/home-and-community based agencies—deliver care across a variety of settings that patients call home. These settings include personal residences, skilled nursing facilities and nursing facilities, assisted living facilities, hospitals, hospice inpatient units, hospice houses, and shelters for those experiencing homelessness. The vast majority of this care is delivered in the community, outside the four walls of a healthcare facility. Most of this care is documented via an Electronic Medical Record (rather than a certified Electronic Health Record (EHR).

The Alliance commends the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) for its commitment to strengthening healthcare cybersecurity. Indeed, we share OCR's concern that the healthcare landscape has changed significantly since the existing Security Rule was implemented. We sincerely support the focus on ensuring the security of electronic protected health information (ePHI) and the information systems that create, receive, maintain, or transmit ePHI. We appreciate the need for tighter processes and procedures around cybersecurity of ePHI and support improvements to the existing Security Rule. After careful consideration of the proposals in the NPRM we offer the following comments:

Compliance Date and Resource Investment

OCR proposes a mandatory compliance timeline requiring implementation within 180 days from the final rule's effective date (60 days after publication), with up to an additional year and 60 days after the date of publication of the final rule in the Federal Register for business associates meeting certain requirements. This is not a realistic timeline even with entities meeting the current Security Rule requirements and does not consider the size or level of resources available to the entity.

Even the largest of our member organizations with substantial resources devoted to technology and security could not meet the proposed timeline. Illustratively, these organizations operate massive, complex networks and must undertake extensive planning, policy, and procedure development and implementation across more than 500 offices while complying with varying state-specific requirements across more than 40 states. Network segmentation and mapping, while seemingly straightforward tasks, are particularly daunting. Segmentation planning alone could take months in organizations of significant size with the configuration taking several more months let alone testing and deployment. Network mapping in a setting that is not contained within the four walls of an institution with technology assets that are changing frequently across numerous offices is nearly impossible. The entire project could not

be completed within the 12 months before it would need to be reviewed and updated again, and it would not be an accurate map as it is constantly changing.

Large organizations with in-house Security Officers (SOs) and expert staff devoted to technology and security systems also state that is not possible to meet the proposed compliance deadline. However, most healthcare entities are medium to small-sized organizations that do not have the in-house expertise and resources to lead the organization through the myriad additional requirements in the timeframe proposed. These organizations will need to contract with a third party to conduct this work. And it may take several contractors to complete it.

The estimated cost of outsourcing varies significantly based on organizational size and security needs. This can range from $50,000 per year in small organizations contracting for compliance policies and procedures, online training and secure IT solutions to over $1M per year for large organizations needing more dedicated security and compliance team members, more detailed security infrastructure and advanced risk assessments. The cost estimates contained in the NPRM assume that entities will primarily be implementing new requirements with existing staff. Small to medium sized providers have consistently stated that they will need to utilize contractors for nearly all additional provisions. In fact, they utilize third party contractors now for some of the existing security requirements. Moreover, the time and cost estimates for those entities utilizing in-house staff in the NPRM are grossly underestimated. For instance, large organizations will need much, much more time than 4.5 hours in the first year to take additional actions that would be required for network segmentation. The time it will take is measured in months not hours and the work will need to be performed by multiple staff not one individual. These additional, unplanned costs could be insurmountable for some providers, especially having to be procured within a short period of time.

It is not just the cost of internal implementation or that of these contractors that is concerning, it is also the vetting necessary. There will undoubtedly be a surge in individuals and companies holding themselves out as experts to assist companies in meeting the NPRM requirements that are finalized. There is concern across the industry that some of those claiming to be experts will not be and perhaps could have the intent of obtaining the ePHI they would have access to. Having Qualified Security Assessors (QSA) for the HIPAA Security Standard as there is for the Payment Card Industry Data Security Standard (PCI DSS) could be of help. The time necessary to develop the education, training and certification for such, however, could not be accomplished within the NPRM compliance timeframe.

Providers will also need to go beyond merely requiring attestations of compliance from their business associates and actively take steps to ensure each business associate's compliance with security requirements. One of the most commonly utilized business associates for home-based providers is an EMR vendor. These vendors, along with other frequently used partners such billing companies and auditors, are fairly easily able to provide SOC 2 reports as evidence of compliance. However, some business associates are individual consultants or small companies that do not routinely obtain SOC 2 reports. It is not clear if the business associates would need to have a SOC 2 Type I or Type II review. Regardless of the type of report required, the cost of such a review will be passed through to the home-based provider, further increasing the financial burden of compliance.

Multi-factor Authentication

As stated above, most of the care provided by Alliance members is provided in the community, much of which occurs in rural areas. Accordingly, clinicians are accessing ePHI in patient homes and documenting care provided while in the home or, as is quite often the case, in their vehicles between visits. It could be difficult to implement MFA in these environments. Specifically, the internet connections in the community are inconsistent and non-existent in some areas, especially rural areas where internet bandwidth is especially limited. The homes of the patients served are often not equipped with an internet connection. Even in skilled nursing and assisted living facilities it is not uncommon that a connection cannot be established through wi-fi or hotspots, as the buildings commonly do not accommodate such technology. Therefore, utilizing a code that needs to be received via email, or a cell phone would not be reliable. Having to purchase hardware security keys adds to the cost burden ($95+ per key).

Clinicians report that they access their devices in patient homes to obtain information necessary for the visit as well as to record some data from their assessments. The nature of caring for patients in the home setting is such that the visit interaction between the clinician and the patient and family is not structured like it is in a clinic or medical office. Rather, clinicians are often 'timed out' of their devices during the visit and must sign in multiple times throughout the visit. It is not clear if the proposed requirements include having to utilize MFA for re-entry after being timed out. Also frequently, clinicians must resort to logging into their devices to document and save such documentation locally on the device until they are able to reach a location with a reliable internet connection so that the documentation can be uploaded to the system. These realities of delivering care in the community raise the question of MFA value versus burden if required each time a clinician accesses the system.

In summary, we believe the intent of this NPRM is on target and fully support this intent. However, as proposed, the requirements would create burdensome, costly and onerous requirements that would not necessarily achieve the intended result. Therefore, we recommend that OCR work with the Alliance and the care at home industry to determine the provisions in this NPRM that would most adequately strengthen the security of ePHI in a manner consistent with the environment in which this care is delivered and at a commensurate cost and resource burden then implement these requirements within a realistic timeline.

Sincerely,

Scott Levy

Scott Levy
Chief Government Affairs officer

State Association Co-signors
Arizona Association for Home Care (AAHC)
Arizona Hospice & Palliative Care (AHPCO)
Association for Home & Hospice Care of North Carolina
California Association for Health Services at Home
Delaware Association for Home & Community Care
Granite State Home Health & Hospice Association
Healthcare Association of Hawaii
Homecare and Hospice Association of Utah
Home Care & Hospice Alliance of Maine
Home Care and Hospice Association of Colorado
Home Care Association of Florida
Home Care Association of New York State
Hospice & Palliative Care Association of Iowa
Hospice and Palliative Care Association of New York State
Hospice & Palliative Care Network of Maryland
Illinois HomeCare & Hospice Council
Indiana Association for Home and Hospice Care
Kansas Home Care & Hospice Association
Kentucky Home Care Association
Minnesota Home Care Association
Ohio Health Care Association
Pennsylvania Homecare Association
South Carolina Home Care & Hospice Association

Tennessee Association for Home Care
Texas Association for Home Care & Hospice
The Connecticut Association for Healthcare at Home
The Wisconsin Hospice and Palliative Care Association
Virginia Association for Home Care and Hospice
VNAs of Vermont
West Virginia Council for Home Care and Hospice
Wisconsin Association for Home Health Care