DRAFT – NOT FOR DISTRIBUTION

March 7, 2025

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

RE: Docket ID number HHS–OCR–0945–AA22

The National Alliance for Care at Home (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, totaling 1500 providers representing 10,000 offices/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 – home health agencies, hospices, palliative care practitioners and organizations, and personal care agencies/home-and-community based agencies - deliver care in numerous settings that patients call home. These include personal residences, skilled nursing facilities/nursing facilities, assisted living facilities, hospitals, hospice inpatient units, hospice houses, and shelters for those experiencing homelessness. The majority of care is delivered in the community - outside of the four walls of a healthcare facility. Most of the care is documented via an Electronic Medical Record (not a certified Electronic Health Record (EHR)). As such, we are grateful for the opportunity to comment

on the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information proposed rule.

The Alliance commends the Office for Civil Right at the U.S. Department of Health and Human Services (HHS) for its commitment to improving healthcare cybersecurity. Indeed, the environment has changed significantly since the existing Security Rule was implemented. We sincerely support the focus on ensuring the security of 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, along with the state associations that have also signed this letter, offer the following comments:

Compliance Date and Resource Investment

A mandatory compliance date of 180 days from the "effective date" (60 days after publication) of a finalized rule is proposed with up to an additional one year and 60 days after 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 regardless of 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. In addition to massive, complex networks these entities must navigate planning and policy and procedure development and implementation across more than 500 offices and coordinate with specific requirements of 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 to outsource ranges 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. The 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 actually 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 requiring attestations of compliance with security requirements from their business associates to ensuring compliance of each business associate. One of the most utilized business associates for providers of care in the home is an EMR vendor. These vendors are fairly easily able to provide SOC 2 reports as evidence of compliance as are most other frequently utilized vendors such as billing companies and auditors. 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, the cost of such review will be passed through to the home care provider adding to the cost burden of compliance.

Multi-factor Authentication

As stated elsewhere in these comments, 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. The homes of the patients served are often not equipped with an internet connection. Even in skilled nursing and assisted living facilities a connection cannot be established through wi-fi or hotspots as the buildings 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,