athenahealth
80 Guest Street
Boston, MA 02135

March 7, 2025

Anthony Archeval
Acting Director, Office of Civil Rights
U.S. Department of Health and Human Services
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 NPRM, RIN 0945-AA22

Submitted electronically via www.regulations.gov

Dear Acting Director Archeval:

athenahealth, Inc. ("athenahealth" or "athena") appreciates the opportunity to respond to the Department of Health and Human Services (HHS) Notice of Proposed Rulemaking (NPRM) on the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information.

Over the past 27 years, athenahealth has built a network encompassing approximately 385,000 healthcare providers in both ambulatory and acute settings across all fifty states. We offer a range of services, including electronic health records (EHR), practice management, care coordination, patient engagement, data analytics, and revenue cycle management, as well as related services, such as Epocrates, to physician practices and hospitals. More than 155,000 providers utilize our single-instance, continuously updated cloud-based platform to serve one-quarter of the U.S. population. We also support on-premises software solutions. In both hosting paradigms, athenahealth strives to establish connections with partners across the care continuum, enabling our clinicians to enhance the quality of care they deliver.

athenahealth has long advocated for the enhanced protection of sensitive health data and agrees that improvements can be made in healthcare to bolster the privacy, security, and protection of electronic protected health information (ePHI). We support OCR's efforts to address evolving threats in the healthcare sector and are pleased to share our perspective on this critical issue. Several challenges must be addressed to ensure that the proposed rule is both effective and implementable. The following commentary outlines our key concerns and recommendations for improvement.

1) HHS Must Allow Reasonable Timelines to Adopt New Requirements

athenahealth is concerned that many of the proposals set aggressive timelines for action that are impractical and do not reflect current operational realities. These timelines significantly underestimate the activities, time, and effort required to meet the proposed compliance deadlines. For instance, the proposal to require a business associate to report to the covered entity the activation of its contingency plan under 45 CFR 164.308(a)(13) "without unreasonable delay, but no later than 24 hours after activation" is not practical. A reasonable window of 36 to 48 hours is necessary to provide businesses with adequate time for reaction and mitigation. We recommend engaging with stakeholders to review each proposal collaboratively, identifying realistic timeframes and streamlining requirements to prevent redundancy and align with current industry best practices.

athenahealth
80 Guest Street
Boston, MA 02135

2) Creation, Maintenance, and Disclosure of the Technology Asset Inventory

athenahealth agrees with OCR that a technology asset inventory is a valuable concept that can enhance security against threats. However, the requirement to develop and maintain a technology asset inventory and a network map illustrating the movement of ePHI throughout the regulated entity's electronic information system on an ongoing basis would impose a significant burden and additional costs, limiting the value of such inventories. OCR should consider the regulatory and financial impacts of implementing this proposal and adjust the proposed requirements accordingly. If finalized, we recommend that the Agency collaborate with stakeholders to develop best practices for maintaining a written technology asset inventory and network map of electronic information systems, including all assets that may affect the confidentiality, integrity, or availability of ePHI.

3) New and Emerging Technologies Request for Information: Artificial Intelligence

The proposed rule notes that a regulated entity's risk analysis must include consideration of the type and amount of ePHI accessed by the AI tool, to whom the data is disclosed, and to whom the output is provided. As part of our risk analysis questionnaire, athenahealth captures the types of data used in AI models (including protected health information) and the number of patients whose data is used in the input data. Given the information already collected, we seek clarity regarding the purpose of requiring both the type and the amount of ePHI to be analyzed. Is the intent to impose more stringent requirements on specific types of ePHI? Maintaining flexibility in the finalized policies will be essential to avoid imposing excessive or unmanageable burdens on healthcare organizations and their technology partners.

We look forward to continuing our collaboration with your team to improve healthcare outcomes. Please do not hesitate to contact me directly at 845-323-3454.

Regards,

Jennifer Michaels
Senior Manager, Government & Regulatory Affairs
athenahealth, Inc.