James L. Madara, MD
CEO, EXECUTIVE VICE PRESIDENT
james.madara@ama-assn.org

July 9, 2021

James Olthoff, PhD
Director
Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: Resource Guide for Implementing the HIPAA Security Rule Call for Comments

Dear Director Olthoff:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to respond to the call for comments (CFC) on the National Institute of Standards and Technology's (NIST) proposed update to NIST Special Publication (SP) 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* ("Resource Guide").

We applaud NIST's interest in making improvements to the Resource Guide and cultivating expanded awareness, applications, and uses for the guide**.** NIST has developed valuable resources that provide guidance on cybersecurity trends and recommend best practices to individuals and organizations across the country, including many physician practices. We greatly appreciate NIST's recognition that cybersecurity practices will vary across organizations, depending on levels of technical understanding, financial and human resources, and risk tolerance. This flexibility allows entities to customize how they adopt and implement a cybersecurity framework. The same principles apply with respect to how organizations implement HIPAA's Security Rule.

NIST's work to update the Resource Guide reflects its commitment to communicating and cooperating with other sectors, federal agencies, and implementers. Specifically, we are pleased that NIST is contemplating ways to provide guidance on "recognized security practices" in light of Public Law 116-321, which requires the Secretary of the Department of Health and Human Services (HHS) to consider certain recognized security practices of covered entities when making certain determinations about HIPAA Security Rule compliance.[1] The AMA advocated for such a policy and believes NIST's guidance to HHS on such matters to be critical. We strongly urge NIST to coordinate with HHS to ensure this Resource Guide includes guidance on what security practices will be recognized by HHS for purposes of Public Law 116-321. Such guidance would be invaluable to the physician community, which has been inundated in recent years by increasing cyber-attacks.

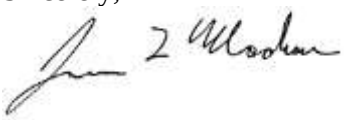
We again note that flexibility will be critical in the health care space where a solo practitioner has very different resources than a large health system. The AMA strives to help physicians navigate a complex

[1] Pub. L. 116-321 (January 5, 2021). Available at https://www.congress.gov/bill/116th-congress/house-bill/7898.

future where non-traditional players, such as cyberhackers, expose their practices and their patients to risk. Yet, while discussions of cybersecurity typically include perspectives of government, health information technology (health IT) vendors, and large health and hospital systems, the physician voice is relatively unheard. We recommend that NIST and others in the cybersecurity space contemplate ways to make cybersecurity best practices affordable, attainable, and approachable for physicians without extensive health IT knowledge or experience.

Thank you for this opportunity to respond to the CFC. We look forward to working further with NIST to ensure that physicians practice good cyber hygiene in the continually evolving technology landscape. If you have any questions regarding our comments, please contact Laura Hoffman, Assistant Director of Federal Affairs, at laura.hoffman@ama-assn.org.

Sincerely,



James L. Madara, MD