From: **Laura Hoffman**
Date: Wed, Apr 5, 2017 at 11:49 AM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Please find attached comment from the American Medical Association on NIST's draft update of its cybersecurity framework.

Thank you,

Laura Hoffman

Laura G. Hoffman, JD
Assistant Director, Federal Affairs
American Medical Association
25 Massachusetts Avenue, NW
Suite 600 Washington, DC 20001-7400

[Attachment Copied Below]

April 5, 2017

Kent Rochford, PhD
Acting Director
Acting Under Secretary of Commerce for
Standards and Technology
National Institute of Standards and Technology
100 Bureau Drive Gaithersburg, MD 20899

Dear Acting Director Rochford:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to respond to the request for comment (RFC) on the National Institute of Standards and Technology's (NIST) proposed update to the Framework for Improving Critical Infrastructure Cybersecurity (the Framework).

We value NIST's ability to identify cybersecurity trends and aggregate best practices, particularly at a time in which patients and physicians regularly interact with health information technology (health IT) both within and outside of physician practices. In particular, we support the Framework's voluntary approach that offers flexibility and allows entities to customize how they adopt and implement a cybersecurity framework. This is critical in the health care space where a solo practitioner has very different resources than a large health system. We appreciate that NIST created and is working to improve a tool through which an organization can evaluate its security practices. **As NIST continues to refine its Framework, we urge it to continue to recognize that cybersecurity requires flexibility, communication, and cooperation among entities and sectors.**

The AMA strives to help physicians navigate a complex 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 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.** Finally, we suggest that NIST consider developing a non-technical, plain-language compendium to accompany the Framework to help individuals champion the importance of cybersecurity to their organization and promote a culture of good cyber hygiene.
Thank you for this opportunity to respond to the RFC. 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.

Sincerely,

James L. Madara, MD