AMA
AMERICAN MEDICAL ASSOCIATION

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

ama-assn.org
t (312) 464-5000

April 15, 2016

Karen B. DeSalvo, MD, MPH, MSc
Acting Assistant Secretary for Health
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, SW, Suite 729-D
Washington, DC 20201

Dear Acting Assistant Secretary DeSalvo:

On behalf of the physician and medical student members of the American Medical Association (AMA), thank you for the opportunity to respond to the request for information (RFI) on updates to the Office of the National Coordinator for Health Information Technology's (ONC) voluntary Personal Health Record (PHR) Model Privacy Notice (MPN).

Patients and physicians are increasingly interacting with health information technology (health IT) without accurate and sufficient information about how their data is used and protected. For this reason, the AMA strongly supports ONC's efforts to inform consumers of how these products, particularly those developed by entities not covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), store, use, and disclose health information. Specifically, the AMA applauds ONC's recognition that the MPN must continue to evolve with the consumer health technology landscape.

We recognize that the MPN is voluntary for personal health application developers (PHADs) and that it will not necessarily contemplate every facet of privacy and security. Nonetheless, we believe that health IT and PHR developers should, at a minimum, have clear privacy policies to ensure accuracy, transparency, and the appropriate level of consumer choice. A study published in the *Journal of the American Medical Association* in March 2016 found that, of the 211 Android-based diabetes apps reviewed, over 80 percent did not have privacy policies.[1] Of those with privacy policies, over 80 percent still collected user data and almost 50 percent shared it.[2] Only four of the apps' privacy policies stated that users would be asked for permission before their data would be shared.[3]

Since personal health applications store, use, and disclose patient health information, the risk to the confidentiality and security of a patient's data is the same as when such information is held by a

[1] Blenner SR, Köllmer M, Rouse AJ, Daneshvar N, Williams C, Andrews LB. Privacy Policies of Android Diabetes Apps and Sharing of Health Information. JAMA. 2016;315(10):1051-1052. doi:10.1001/jama.2015.19426, available at http://jama.jamanetwork.com/article.aspx?articleid=2499265.
[2] Id.
[3] Id.

physician—if not magnified—due to the lack of app privacy and security standards. Patients must always be made aware of how their personal and often sensitive health information is used and shared. In addition, physicians do not have the information they need to be able to understand how various health apps protect privacy. This can result in hesitance to recommend such products to patients thereby limiting the potential for patients to improve and maintain their health status through the use of otherwise beneficial technology.

Accordingly, the AMA believes that the standards to which developers of personal health applications are held should move toward the same standards to which physicians are held, resulting in an MPN that closely tracks HIPAA's Notice of Privacy Practices (NPP). In response to the RFI's specific questions, the AMA submits the following comments:

In Question 1 of the RFI, ONC asks what types of health technology developers could and should use an updated voluntary MPN. **The AMA recommends that all PHADs should utilize an updated MPN, especially since they are not currently covered by HIPAA**. Examples include developers of mobile health or wellness applications, personal health records, and telemedicine products and applications. Additionally, while not specifically tied to health care, companies that manage applications and services in the cloud on behalf of PHADs could also use an updated MPN to educate customers on their hosting practices. These recommendations reflect guidance issued by the Federal Trade Commission (FTC), which reviewed consumer concerns with mobile devices and recommended that all application developers have privacy policies and include references to such policy when submitting the tool to an operating system provider.[4] As noted in the FTC report, such a policy would not deter market participation but would enhance consumer trust that is vital to expanding the use of these products.[5]

In Sections 2 and 3, ONC asks what information types should be considered in and out of scope for the MPN and what types of practices involving such information should be included. **The AMA recommends that all information that could be used to identify an individual be included in the MPN.** This should encompass information that is typically covered by an NPP—i.e., information collected by a personal health application related to the past, present, or future physical or mental health or condition of an individual; the provisions of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. It should also, as ONC suggests in its RFI, include names, account access information, credit card numbers, IP address information, social security numbers, telephone numbers (cell and landline), global positioning system (GPS) or geo-location data, data about how a consumer's body functions ranging from heart rate to menstrual cycle, and genomic data.

The AMA agrees with ONC that the types of practices that could be in scope for the MPN include sale of data, including geo-location data; sale of anonymized or de-identified data, with or without restrictions on re-identification; sale of identifiable data; sale of statistics aggregated from identifiable data; use of data by the original collector to market products to the consumer; allowance of third parties to use the data for marketing purposes; allowance of government agencies to access the data, and for what purposes (such as law enforcement or public health); allowance of researchers at academic and non-profit institutions to

[4] Federal Trade Commission. Mobile Privacy Disclosures: Building Trust Through Transparency. February 2013. Available at https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf

[5] Id.

access either identifiable or de-identified data; access to the data by employers, schools, insurance companies or financial institutions with or without the consumer's consent; and retention or destruction of consumer data when the relationship between the PHAD and consumer terminates. We again urge that, where possible, these policies closely track current HIPAA requirements to minimize confusion and build off of current expectations.

In Section 4, ONC asks what privacy and security issues consumers are most concerned about when their information is collected, stored, or shared. Our experience has shown that patients are deeply concerned about the release and unauthorized access of their health information but are largely unaware of the risks present in new technology. As the FTC notes, this lack of transparency has created confusion and misconceptions for consumers that, at times, has required the agency to take enforcement action.[6] In particular, patients have noted that they want to have a choice in the type of information that is used and collected by applications and how their data is stored, accessed, and disclosed. Patients have also noted that health IT tools should limit the collection of personal health data to that which is necessary for the operation of the application—for example, a tool that monitors a specific condition may not need to know a patient's entire medical history. **To address these concerns, we believe the MPN should include specific sections that outline how data is collected, used, and disclosed. Patients should also have a clear right to access the data, request additional privacy protections, and note complaints to a PHAD.** Again, this not only provides transparency but also ensures consistency with existing HIPAA requirements, aligning expectations across the health care industry.

In Section 5, ONC asks what information the MPN should convey to the consumer regarding specific security practices and what level of detail is appropriate for a consumer to understand. We recommend that the MPN convey whether the information is encrypted when it is at rest (including both the consumer's device and where it is stored on the PHAD's end, if applicable, such as in the cloud) and whether it is encrypted in transit. An appropriate level of detail regarding the strength of data encryption should be required. Consumers are becoming more adept at understating the need for strong encryption and have greater access to this level of information under the "help" or frequently asked question pages on social networking or online retail sites. Furthermore, this level of detail should also be specific enough that consumers can identify the security capabilities between methods available to access or transmit their data. For instance, the MPN should clearly convey any differences and the levels of security when a consumer accesses their data through a mobile app versus a web browser, or in instances when a consumer directs a PHAD to send their data to another PHAD. **In general, developers should not only have and provide consumers with privacy policies, but these policies should be standardized**. This ensures that information is clear and comprehensive and that different tools can be readily compared. ONC should require MPNs to follow uniform components and language, similar to existing NPPs, to easily convey terms that are often technical in nature.

In Section 8, ONC asks how the MPN should describe a consumer's ability to retrieve or move their data when the relationship between the consumer and the health technology developer terminates**. We suggest that the MPN inform a consumer what will happen to the consumer's data once the consumer has deactivated his/her account, using options similar to those available to business associates:** (1) retain

[6] See e.g., *United States v. Path, Inc.*, No. C13-0448 (N.D. Cal. Jan. 31, 2013) (proposed consent order), available at http://www.ftc.gov/os/caselist/1223158/index.shtm. In the Matter of Frostwire LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 12, 2011) (consent order), available at http://www.ftc.gov/os/caselist/1123041/index.shtm.

only that health information which is necessary for the developer to continue its proper management and administration or to carry out its legal responsibilities; (2) destroy the remaining health information that the developer still maintains in any form; and (3) if destruction of the health information is not possible, a commitment from the developer to not use or disclose the information to any third party. Consumers should also be notified when an entity changes its privacy practices, and not just when a relation is terminated.

We greatly appreciate the ONC's efforts to assist consumers and physicians alike with a more transparent understanding of how patient health information will be stored, used, and disclosed by PHADs. While we recognize that the MPN is voluntary and not all uses of patient health information will necessarily be disclosed, we believe the MPN to be a step in the right direction towards improved privacy and security of personal health applications.

The AMA looks forward to working further with ONC to ensure that patients and physicians know how PHADs plan to protect the confidentiality and security of patient protected health information in the continually evolving technology landscape. If you have any questions regarding our recommendations, please contact Laura Hoffman, Assistant Director of Federal Affairs, at 202-789-7414 or laura.hoffman@ama-assn.org.

Sincerely,

[Signed]

James L. Madara, MD