AMA
AMERICAN MEDICAL ASSOCIATION

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

ama-assn.org

December 20, 2018

The Honorable Walter G. Copan
Director
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Dear Dr. Copan:

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 information (RFI) on the National Institute of Standards and Technology (NIST) developing a Privacy Framework ("Framework"). Given the concerns about how information technology (IT) may affect privacy at individual and societal levels, the AMA applauds NIST's efforts. Overall, the AMA believes that the Framework should introduce how privacy risk management could be used to create more trustworthy IT systems.

The AMA's approach to privacy is governed by our Code of Medical Ethics and long-standing policies adopted by our policymaking body, the House of Delegates, which support strong protections for patient privacy and, in general, require physicians to keep patient medical records strictly confidential. AMA policy and ethical opinions on patient privacy and confidentiality provide that a patient's privacy should be honored unless waived by the patient in a meaningful way, de-identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of patient privacy or breaches of confidentiality. When breaches of confidentiality are compelled by concerns for public health and safety, those breaches must be as narrow in scope and content as possible, must contain the least identifiable and sensitive information possible, and must be disclosed to the fewest possible to achieve the necessary end.

The AMA's policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the patient-physician relationship. This is particularly important in scenarios involving sensitive health information. For example, in the mental health arena, striking the correct balance is critical in encouraging individuals with mental illness and/or substance use disorders to seek treatment. Privacy risks include re-identification of patients through de-identified (or partially de-identified) data, misunderstanding or disregard of the scope of a patient's consent, patient perception of loss of their privacy leading to a change in their behavior, embarrassment or stigma resulting from an unwanted disclosure of information or from fear of a potential unwanted disclosure, perceived and real risks of discrimination including employment and access to or costs of insurance, and law enforcement accessing data repositories beyond their intended scope.

Challenges for Improving Privacy Protections and Developing a Cross-Sector Framework for Privacy[1]

The AMA believes that one of the challenges in improving privacy protection and developing a framework for privacy is complying with numerous federal and state privacy and security requirements. While physicians are covered entities under the Health Information Portability and Accountability Act (HIPAA), and are therefore subject to HIPAA's requirements, penalties, and enforcement actions, physicians use tools that are not covered by HIPAA and may have different privacy and security standards. For example, physicians use medical devices that are overseen by the U.S. Food and Drug Administration's regulation and guidance, yet the electronic medical information created by these devices that is entered in a physician's electronic health record (EHR) system is regulated by the Office of Civil Rights (OCR).

Physicians also have patients who use medical applications (apps) that transmit protected health information and/or connect with the physician's EHR. These apps are often within the purview of the Federal Trade Commission as opposed to OCR, which oversees HIPAA. This raises questions about how physicians should navigate the protected health information that flows from a physician's practice to a patient's app and back to the physician's EHR. Furthermore, if a patient's app is not secure, the information could introduce security vulnerabilities to the physician's health information technology network. It is becoming increasingly unclear to both physicians and patients how, when, and which privacy and security regulations pertain to apps and an individual's information. With the increasing use of open application programming interfaces and of apps by patients to access their health information, the Framework should provide consistent, thoughtful, and holistic guidance so that physicians understand how to mitigate privacy risk and keep their patient's information confidential.

The AMA believes that another challenge in developing the Framework is the treatment and identification of sensitive data and how that definition of "sensitive data" may differ by individual. Specifically, the framework should consider how individuals may differ in how they regulate and control information they consider private and confidential. If a physician is not aware of, or does not contemplate, a patient's desires regarding privacy expectations, the medical encounter can be counterproductive for patients and physicians alike. Thus, the framework needs to contemplate how to handle individual differences in the treatment of their information.

Relatedly, the Framework should prioritize and support methods that enable individuals and entities to protect and securely share pieces of information on a granular, as opposed to document, level. In the health sector, physicians often need to send certain types of health information, or a section of a medical record, without sending the entire record. In fact, sometimes this is required by HIPAA (in other words, sending a "minimum necessary" amount of information), or by state law. Any information disclosed should be limited to that information, portion of the medical record, or abstract necessary to fulfill the immediate and specific purpose of disclosure.

Another challenge with privacy protection is determining the boundary of a data system. Privacy issues can arise at any location where data is processed, including collection, creation, analysis, use, storage, distribution, disclosure, or disposal. The boundary of a data system is related to the scope of authorization

[1] Topics 1 and 2 of the NIST RFI.

and potential liability for operating the system. Stages of data processing, however, may occur outside of this authorization scope that give rise to privacy concerns in the system. The draft Framework should address these issues and provide best practices to determine where one system ends, and another begins.

Minimum Set of Attributes for the Privacy Framework[2]

The AMA appreciates and supports all seven minimum attributes of the Framework. The third attribute (i.e., being adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses) is especially important. The AMA agrees that the Framework should be scalable to organizations of all sizes and be platform- and technology-agnostic and customizable. The Framework should not create unnecessary or disproportionate burden on solo proprietors or small businesses. Many solo practitioners and small group practices must devote their limited resources to addressing immediate demands of clinical practice and clinical care and do not have the resources to hire an employee to focus on managing privacy risk. Moreover, small practices find it more difficult to find the time and expertise to analyze privacy risk and adjust their practices accordingly.

We also support the draft Framework's voluntary approach that offers flexibility and allows entities to customize how they adopt and implement a privacy framework. This is critical in the health care space where a solo practitioner has very different resources than a large health system. As NIST continues to develop its Framework, we urge it to continue to recognize that the Framework requires flexibility, communication, and cooperation among varying entities, sectors, and federal agencies.

Current Requirements and Mandates[3]

In the health care sector, the current regulatory and regulatory reporting requirements are too focused on physician measurement or compliance. Instead, the requirements should be focused on developing positive incentives to adopt better privacy and security practices, communicating the reasons for the requirements and how they are connected to patient care, and ensuring that implementation of the requirements integrates into the workflow and does not add additional unnecessary administrative burden. Thus, while voluntary, the Framework should not take an overly complex approach focused on process measurements and reporting.

The Framework should also strive to identify the practical needs of data controllers (e.g., physicians), goals that are understandable and achievable, and areas with potential high impact, such as, protocols for data segmentation. Moreover, any requirement in the Framework should be clear, concise, and provide meaningful change. For example, requiring an organization to issue a Notice of Privacy Practice that is not comprehendible by individuals or ignored does not promote privacy or reduce risk.

Role of Standards and Standard-Setting Organizations[4]

The AMA believes that if standards play a role in this discussion, it should focus on the principles for standard development. These principles include having the clinical community involved early in the

[2] Topic 8 of the NIST RFI.
[3] Topics 11 and 12 of the NIST RFI.
[4] Topic 13 of the NIST RFI.

process and any standard should be pilot tested in a real-world environment. Moreover, a key principle is measuring the effectiveness of a standards use and ensuring a feedback loop to inform version maturation. The evolution of standard's is best informed by incorporating real-world end-user experiences using an iterative approach. As privacy is a multifaceted issue, privacy standards must focus on a specific outcome or a set of goals aligned with the needs of end users. As a principle of building confidence and adoption, the AMA recommends NIST take in consideration how standards are developed. This should include the process for cross-stakeholder inclusion and efforts by standards development organizations to educate the end-user community.

Organizational Construct for the Privacy Framework[5]

AMA appreciates that NIST is interested in understanding how to structure the Framework to achieve the desired set of attributes and improve integration of privacy risk management processes with the organizational processes for developing products and services for better privacy outcomes. In considering the Framework, NIST should account for the sensitivity of the data and that certain personal data requires greater protection which, if improperly disclosed, could result in a variety of potentially negative consequences for the patient.

Identifying Core Privacy Practices

NIST is interested in identifying core privacy practices that are broadly applicable across sectors and organizations. In the health sector, many of the listed practices are used including de-identification, encryption, and data management. While it may fall within the broad category of data management, **a core privacy practice in the health sector is consent.** Patients typically divulge information to their physicians chiefly for the purposes of diagnosis and treatment. If other uses are to be made of the information, patients should first be given the opportunity to provide their uncoerced permission after being fully informed about the purpose of such disclosures. For example, employers and insurers should be barred from unconsented access to identifiable medical information in case knowledge of sensitive facts form the basis of adverse decisions against individuals. In fact, employers and health insurers are barred from accessing genetic/genomic information under the Genetic Information Nondiscrimination Act and making adverse determinations. Furthermore, marketing and commercial uses of identifiable patients' medical information may violate principles of consent and patient confidentiality.

Inapplicable Practices[6]

The AMA urges caution around disassociability in certain contexts in health care. Disassociability focuses on enabling a data system to process personal information or events without association to individuals or devices beyond the system's operational requirements. This decoupling "blinds" an individual's identity or activities from undue exposure, thus actively protecting that individual from privacy risk. In the practice of medicine, data systems may need to associate personal information to a patient or a patient's device. Otherwise, care may be negatively impacted. Thus, the disassociability privacy engineering objective as a use of cryptographic technology may not be appropriate in the health care industry.

[5] Topic 18 of the NIST RFI.
[6] Topic 23 of the NIST RFI.

Privacy Practices Relevant to New Technologies[7]

The AMA believes privacy practices are relevant for new technologies like the Internet of Things, artificial intelligence,[8] and genomic sequencing.[9] Specifically, proper data management and enabling users to have a reliable understanding about how information is being collected, stored, used, and shared should be adopted. While the types of data items are not new, these technologies provide greater potential access of those data items to other individuals or entities. Thus, there are many new uses for and ways to analyze the collected data, which may raise significant privacy issues. Accordingly, the Framework should discuss how to address these concerns and to incorporate privacy considerations as a part of the development process of any new technology.

Lastly, with proper protections in place, the Framework should also promote data access, including open access to appropriate machine-readable public data, development of a culture to sharing data with external partners, and explicit communication of allowable use with periodic review of informed consent. In providing open access to appropriate data, the AMA encourages disclosure of the characteristics of the datasets, including the data sources, data collection, data model, and data curation methods, accompanied by an assessment of potential biases resulting from the data-gathering process and any efforts made to mitigate these risks. Accounting for unintended bias in data sets is a central metric of data quality and a key to mitigating the risk of potentially furthering disparities.

The AMA appreciates the opportunity to provide comments and thanks NIST for considering our views.

Sincerely,

James L. Madara, MD

[7] Topic 25 of the NIST RFI.

[8] AMA policy addresses privacy issues broadly in the context of AI which the AMA and other major technology stakeholders have coined as augmented intelligence.

[9] It is not possible to de-identified genomic information and even partial capture of genetic information can be used to re-identify individuals.