STATEMENT

of the

American Medical Association

to the

Federal Trade Commission

Re: Intersection of Big Data, Privacy, and Competition

January 7, 2019

The American Medical Association (AMA) appreciates the opportunity to present our views to the Federal Trade Commission (FTC) on the intersection of big data, privacy, and competition. As the largest professional association for physicians and the umbrella organization for state and national specialty medical societies, the AMA is interested in exploring this intersection and its impact on patient care.

Privacy Laws and Regulations Impact on Competition

In the health care sector, state and federal privacy laws may negatively affect competition and innovation because the current regulatory reporting requirements are focused on physician measurement or compliance. Instead, the requirements should be focused on developing positive incentives to adopt better privacy, security, and data 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.

The AMA believes that one of the challenges with big data and 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 FTC 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 (APIs) and of apps by patients to access their health information, FTC should provide consistent, thoughtful, and holistic guidance so that physicians understand how to mitigate privacy risk and keep their patient's information confidential.

Policy Recommendations that Facilitate Competition

The AMA believes that any FTC policy or guidance should be adaptable to many different organizations, technologies, sectors, and uses to promote competition. Moreover, such policy should be scalable to organizations of all sizes and be platform- and technology-agnostic and customizable. Big data and privacy issues 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 big data or privacy concerns. Moreover, small practices find it more difficult to find the time and expertise to analyze big data and adjust their practices accordingly.

Relatedly, it is critical that FTC address the digital or big data divide between those who have the necessary resources and infrastructure to analyze large data sets and those who do not. The AMA believes that if physicians are unable to properly engage with digital medicine and big data, physicians will not be able to support many underserved populations in the United States who will need quality medical care.

Furthermore, to facilitate competition, FTC should promote data access, including open access to appropriate machine-readable public data, development of a culture that informs consumers on the potential benefits and risks of 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.

Presence of Personal Information

The AMA strongly believes that both the presence of personal information and privacy concerns should inform competition analysis. Privacy and competition are becoming increasingly connected. The AMA's approach to privacy is governed by our Code of Medical Ethics and longstanding 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, deidentified, 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 between data sharing and patient privacy 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.

We appreciate the opportunity to provide our comments on big data, privacy, and competition, and look forward to working with the FTC on this and other relevant topics.