STATEMENT

of the

American Medical Association

to the

Federal Trade Commission

Re: The FTC's Approach to Consumer Privacy

May 31, 2019

Division of Legislative Counsel

(202) 789-7426

STATEMENT

of the

American Medical Association

to the

Federal Trade Commission

Re: The FTC's Approach to Consumer Privacy

May 31, 2019

The American Medical Association (AMA) appreciates the opportunity to present our views to the Federal Trade Commission's (FTC) approach to consumer privacy. As the largest professional association for physicians and the umbrella organization for state and national specialty medical societies, the AMA has a vested interest in the privacy of consumer health data, the ability of consumers to make informed choices about data collection and use, and the adequacy of existing legal and self-regulatory frameworks to protect consumers. AMA policy and ethical opinions on patient privacy and confidentiality state 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. These policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the trust inherent in the patient-physician relationship.

General Questions

Actual and Potential Benefits of Information Collection, Sharing, Aggregation, and Use

Actual and potential benefits for consumers include promoting care coordination and value-based care, managing disease outbreaks and other public health concerns, advancing patient engagement and care, improving health care operational efficiency, reducing fraud and enhancing security, preventing readmissions and unnecessary emergency room visits, and finding cures for rare diseases.

Actual and Potential Risks of Information Collection, Sharing, Aggregation, and Use

Actual and potential risks for consumers 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 (or actual) 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.

Sensitivity of Data and Consumer Privacy Preferences

Privacy protections may vary depending on the type of data in question. Health care information is one of the most personal types of information an individual can possess and generate—regardless of whether it is legally defined as "sensitive." The treatment and identification of "sensitive data" and how that term is defined may differ by individual. Specifically, consumer privacy preferences may differ in how they regulate and control information they consider private and confidential. Patients typically divulge

information to their physicians chiefly for the purposes of diagnosis and treatment. Before the information is used for any other purpose, patients should be given the opportunity to provide their uncoerced permission after being fully informed about the purpose of such disclosures. 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, we urge the FTC to contemplate how to handle individual differences in the treatment of consumers' information.

Relatedly, the FTC 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 Health Insurance Portability and Accountability Act of 1996 (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 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 FTC should address these issues and provide best practices to determine where one system ends, and another begins.

Questions About Legal Frameworks

Potential Federal Privacy Legislation

The first step of any ultimately successful privacy framework, legislative or regulatory, places the patient first. Each entity seeking access to patients' most confidential medical information must pass the stringent test of showing why its professed need should override individuals' most basic right in keeping their own information private. Moreover, citizens deserve a full and open discussion of exactly who wants their private medical information and for what purpose.

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. These policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the trust inherent in the patient-physician relationship.

The AMA believes that any potential federal privacy legislation should be adaptable to many different organizations, technologies, sectors, and uses to promote competition. Moreover, such legislation 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 and their patients. 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 difficult to find the time and expertise to analyze big data and adjust their practices accordingly.

Relatedly, it is critical that any privacy legislation 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 because of the lack of access to care or treatment.

Furthermore, to facilitate competition, potential privacy legislation should promote data access, including open access to appropriate machine-readable public data, while prioritizing the development of a culture that informs consumers on the potential benefits and risks of sharing data with external partners, explicit communication of allowable use with periodic review of informed consent, and protections against using data to deny or limit access to coverage. 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.

In the health care sector, the current regulatory and regulatory reporting requirements are too focused on physician measurement or compliance. Instead, any potential privacy legislation 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, any legislation should not take an overly complex approach focused on process measurements and reporting.

Any potential privacy legislation 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 potential legislation 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, is less than fully transparent, or is ignored does not promote privacy or reduce risk.

Gaps in Current Privacy Laws

The AMA believes a gap exists in federal privacy law with the access and use of health information outside the application of HIPAA. While the FTC generally has jurisdiction over this area as a potential deceptive trade practice, the AMA believes that more may need to be done to protect consumer's health information, including enhanced coordination between the FTC and other federal agencies promulgating regulation around data access, use, and exchange.

For example, the AMA is concerned consumer-facing apps will monetize patient data without patient knowledge; this concern has been exacerbated by the Office of the National Coordinator for Health Information Technology's (ONC) recently proposed rule on interoperability and information blocking. The proposed rule requires certain entities, including physicians, to provide consumers with their health information using an app of their choice. The AMA has long heralded the benefits of both application programming interfaces (APIs) and apps to both patients and physicians. Together they can offer better information usability, providing an enhanced view into a patient's medical record repository. However, patient privacy is of utmost concern when non-covered HIPAA entities such as apps gain access to medical information. **To be clear, the AMA supports patients' access to their entire record.** But there is a significant lack of attention on consumer education and patient control over the use of their information once his or her information has been downloaded onto a smartphone. Apps often do not

provide patients with clear terms of how his or her data will be used. The app's terms can be 6,000+ words in length, and can shield a developer's activities by permitting a "royalty-free, perpetual, and irrevocable license, throughout the universe" to "utilize and exploit" an individual's de-identified personal information for scientific research and "marketing purposes." The terms may also permit a developer to "sell, lease or lend aggregated Personal Information to third parties."[1]

Many apps, particularly free apps, use advertisements to generate revenue. The advertisements collect and share an individual's advertising ID—a string of numbers and letters that identify an individual and keep a log of his or her clicks, searches, purchases, and sometimes geographic location as he or she moves through various apps.[2] While the information is often deemed anonymous, the information can be "shockingly easy to de-anonymize, and that hundreds of apps collect 'anonymous' real-time location data that needs only the slimmest additional context clues to tie to an individual person."[3] As National Public Radio and ProPublica report, "it isn't hard to understand the appeal of all of this data to insurers."[4]

A recent *Wall Street Journal* report exposed just how much is at stake when patients share their personal health information with apps. Several apps feed users' personal health information to Facebook even if the individual does not have Facebook installed on his or her phone, or even possess a Facebook account.[5] A study published in the *Journal of the American Medical Association (JAMA)* found that many health apps created to track a user's progress in battling depression or quitting smoking are sharing the personal details they collect about an individual with third parties—like Google and Facebook—without the individual's knowledge or informed consent:

> Transmission of data to third-party entities was prevalent, occurring in 33 of 36 top-ranked apps (92%) for depression and smoking cessation, but most apps failed to provide transparent disclosure of such practices. Commonly observed issues included the lack of a written privacy policy, the omission of policy text describing third-party transmission (or for such transmissions to be declared in a nonspecific manner), or a failure to describe the legal jurisdictions that would handle data. In a smaller number of cases, data transmissions were observed that were contrary to the stated privacy policies.[6]

---

[1] Drew Harwell, Washington Post, *Is your pregnancy app sharing your intimate data with your boss?* (April 10, 2019), available at https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.3b82122fec27

[2] Kaitlyn Tiffany, Vox Media Network, *Angry Birds and the end of privacy* (May 13, 2019), available at https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush

[3] Kaitlyn Tiffany, Vox Media Network, *Angry Birds and the end of privacy* (May 13, 2019), available at https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush

[4] Marshall Allen, National Public Radio, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates* (July 17, 2018), available at https://www.npr.org/sections/health-shots/2018/07/17/629441555/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates ("Merging information from data brokers with people's clinical and payment records is a no-brainer if you overlook potential patient concerns. Electronic medical records now make it easy for insurers to analyze massive amounts of information and combine it with the personal details scooped up by data brokers. Some insurance companies are already using socioeconomic data to help patients get appropriate care, such as programs to help patients with chronic diseases stay healthy. Studies show social and economic aspects of people's lives play an important role in their health. Knowing these personal details can help them identify those who may need help paying for medication or help getting to the doctor. … But experts said patients' personal information could still be used for marketing, and to assess risks and determine the prices of certain plans.")

[5] https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

[6] Kit Huckvale et al., JAMA Netw Open. 2019;2(4):e192542, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation* (April 19, 2019), available at https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=041919

Apps are also being used as a powerful monitoring tool for employers and payers. Couched in corporate wellness, employers and payers have aggressively pushed to gather more data about their employees' lives than ever before.

> Experts worry that companies could use the data to bump up the cost or scale back the coverage of health care benefits, or that women's intimate information could be exposed in data breaches or security risks. Although the data is made anonymous, experts also fear that the companies could identify women based on information relayed in confidence, particularly in workplaces where few women are pregnant at any given time.[7]

Not only do these practices jeopardize patient privacy and commoditize an individual's most sensitive information, but they also threaten patient willingness to utilize technology to manage their health—a goal frequently expressed by the administration. In fact, a Rock Health 2018 National Consumer Health Survey found that just 11 percent of respondents said they would be willing to share health data with tech companies.[8]

The survey noted that physicians are the most trusted entities with whom patients are willing to share information. However, it notes, confidence is dropping, possibly due to spillover from privacy and security breaches in other sectors and general distrust of "big tech."[9] A 2017 Black Book survey reports that:

- 87 percent of patients were unwilling to comprehensively share all of their health information with their physicians;
- 89 percent of consumers who had visited a health care provider in 2016 said they had withheld some information during their visits;
- 81 percent were concerned that information about chronic conditions was being shared without their knowledge; and
- 99 percent were concerned about the sharing of mental health notes.[10]

In other words, carelessness and lack of transparency in how consumer information is handled and used by technology has likely influenced what a patient is likely to share with his or her physician. This should serve as a warning to policy makers that consumers take privacy very seriously. **Privacy safeguards must be established concurrently with any health information exchange policies—particularly when consumer-facing technology is implicated—or patient health and safety will be jeopardized.**[11]

---

[7] Drew Harwell, Washington Post, *Is your pregnancy app sharing your intimate data with your boss?* (April 10, 2019), available at https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.3b82122fec27

[8] Sean Day and Megan Zweig, Rock Health, *Beyond Wellness for the Healthy: Digital Health Consumer Adoption 2018*, available at https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/

[9] Sean Day and Megan Zweig, Rock Health, *Beyond Wellness for the Healthy: Digital Health Consumer Adoption 2018*, available at https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/

[10] Black Book Market Research, *Healthcare's Digital Divide Widens* (Jan. 3, 2017), available at https://blackbookmarketresearch.newswire.com/news/healthcares-digital-divide-widens-black-book-consumer-survey-18432252

[11] "Incomplete medical histories and undisclosed conditions, treatment or medications raises obvious concerns on the reliability and usefulness of patient health data in application of risk based analytics, care plans, modeling, payment reforms, and population health programming." Doug Brown, Black Book Managing Partner, available at https://www.prnewswire.com/news-releases/healthcares-digital-divide-widens-black-book-consumer-survey-300384816.html

We believe the FTC can use its expertise in this area to help other agencies consider potential privacy risks posed by entities not covered by existing privacy law. It can also weigh in on potential policy mechanisms that would aid the FTC in its enforcement activities. Using the example above, ONC could include in its final rule on interoperability and information blocking the requirement that, as part of an electronic health record (EHR) vendor's certification, ONC should require the EHR check whether an app attests whether it has adopted (1) industry-recognized development guidance; (2) transparency statements and best practices; and (3) a model notice to patients. We also believe this could act as a "bookend"—placing app developers between ONC health IT certification requirements (which would be imposed on EHR vendors), and FTC's enforcement of unfair and deceptive practices. In other words, an app developer would be strongly motivated to attest "yes" and to act in line with their attentions.

We appreciate the opportunity to provide our comments and look forward to working with the FTC on this and other relevant topics. Consumer and patient trust in the health care system can only be assured when all entities that maintain a consumer's health information have an obligation to maintain the confidentiality of that information and when patients truly have autonomy and control over decisions to disclose or retain their personal information.