AMA
AMERICAN MEDICAL ASSOCIATION

JAMES L. MADARA, MD
EXECUTIVE VICE PRESIDENT, CEO

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

August 20, 2020

The Honorable Joseph J. Simons, JD
Chairman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Federal Trade Commission: Health Breach Notification Rule, 16 CFR part 318, Project No. P205405

Dear Chairman Simons:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to submit comments in response to the U.S. Federal Trade Commission's (FTC) request for public comment on its Health Breach Notification (HBN) Rule ("HBN Rule" or "Rule"). The FTC seeks to ensure the Rule has "kept up with changes in the marketplace, technology, and business models," noting that "as consumers turn towards direct-to-consumer technologies for health information services (such as mobile health applications, virtual assistants, and platforms' health tools), more companies may be covered by the FTC's Rule." The AMA greatly appreciates the FTC's recognition of shifts in the technologies patients use to manage their health care and information, particularly following the passage of the 21st Century Cures Act[1] (Cures) and its implementing regulations promulgated by the Office of the National Coordinator for Health Information Technology[2] (ONC) and the Centers for Medicare & Medicaid Services[3] (CMS) earlier this year. **As health information is increasingly exchanged outside of the protections of the Health Insurance Portability and Accountability Act (HIPAA), the FTC must continue to serve a critical role in preserving and strengthening the privacy and security protections of consumers' health information. The Rule is more important now than ever and we strongly urge the FTC to expand its scope and enforcement.**

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. 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. Patient trust in the health care system can only be assured when all entities that maintain a patient's health information have an obligation to maintain the confidentiality of that information and

[1] Public Law 114 – 255, 130 Stat. 1033 (2016).
[2] 45 CFR parts 170 and 171.
[3] 42 CFR Parts 406, 407, 422, 423, 431, 438, 457, 482, and 485; 45 CFR Part 156.

when patients truly have autonomy and control over decisions to disclose or retain their personal information. The AMA's recommendations for how to strengthen privacy guardrails and foster greater trust are included below.

The FTC Should Expand the Scope of the HBN Rule Beyond Traditional Personal Health Records (PHRs)

Currently, the Rule's breach notification obligations extend to PHRs, defined as electronic records of identifiable health information that can be drawn from multiple sources and that are managed, shared, and controlled by or primarily for the individual. These obligations stem from Congress' recognition in 2009 that certain entities—namely, vendors of PHRs and PHR-related entities such as those that offer products and services through PHR websites, access information held by PHRs, or send information to PHRs—collected individuals' health information yet were not subject to the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Generally speaking, the HBN Rule requires PHRs and PHR-related entities to provide notice to consumers whose unsecured individually identifiable health information has been breached, in addition to providing notice to the FTC and, in some cases, the media. The Rule also requires third-party service vendors to provide notice to PHR vendors and PHR-related entities of breach discoveries.

U.S. health care has gradually shifted over the last 10 years toward digital record-keeping in the professional health care realm—the world of hospitals, health plans, and physician practices. That transition occurred under the umbrella of privacy and security rules rooted in HIPAA, a law which predates most modern online and mobile services, and explicitly excludes health information created or managed by patients themselves or by third-party apps—the very content the Rule seeks to protect. **The rapid growth in the range and volume of digital patient data beyond the confines of the HIPAA framework—and exchanged using technologies and platforms beyond PHRs—merits serious attention.** For many patients, the mobile nature and ease of use of third-party apps make them more attractive than traditional PHRs as a way to manage their health records. The AMA expects patients will continue to shift from PHRs to mobile health apps or PHR-health app hybrids going forward. Absent clear guardrails around how entities like app developers use data, public trust will crumble in the face of repeated scandals and undermine the potential for digital health to facilitate an era of more accessible, coordinated, and personalized care.

We learn more each day that personal health information is no longer private. Social media platforms, wearable fitness trackers, and apps allowing patients to download health records from EHRs and manage health conditions all collect data that are not protected by HIPAA. That means these data can be shared for a wide range of purposes, including advertising and marketing. Sharing that health information with data brokers, who can combine it with other consumer information (such as credit score, level of education, and even something as simple as a zip code), creates the perfect recipe for harmful profiling and discrimination.[4] Data mining by insurers and employers leads to the creation of health or "risk" scores, which can result in harmful profiling and discrimination. Social media platforms, Internet search engines, wearable fitness trackers, and applications (apps) to manage pregnancy and mental health all pool personal data, turning it into a valuable commodity.

[4] Favaretto, M., De Clercq, E. & Elger, B.S. Big Data and discrimination: perils, promises and solutions. A systematic review. *J Big Data* 6, 12 (2019). https://doi.org/10.1186/s40537-019-0177-4.

Indeed, there is growing awareness of how companies monetize individuals' health and other personal information. A 2019 Morning Consult national survey showed that 94 percent of people feel privacy and security of their medical information is important,[5] while a 2019 study by Rock Health and Stanford's Center for Digital Health shows consumers have become more reticent to share their health data.[6] Among health care stakeholders, consumers are most willing to share their health data with physicians, but that sentiment has slipped since 2017, possibly due to spillover from privacy and security breaches in other sectors and general distrust of "big tech."[7] 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.[8]

In other words, carelessness and lack of transparency in how consumer information is handled and used by technology has likely influenced what information a patient shares with his or her physician. **This should serve as a warning to policymakers that consumers take privacy very seriously and that privacy safeguards for consumer-facing technology is critical to preserving patient health and safety.**[9]

Recent events have highlighted not only how critical it is to have clear rules of the road with respect to data use, but also the lost opportunities for progress absent such rules. For example, we are currently experiencing unprecedented reliance on remote care technologies like telehealth to help people avoid leaving their homes during the COVID-19 pandemic. But both patients and clinicians are justified in questioning how platforms will secure and protect the information exchanged during the virtual visits. Similarly, many private and public efforts are underway to collect, use, and disseminate public health surveillance data to help inform public health officials and policymakers about the spread of the novel coronavirus. These efforts are critically necessary but have thus far provided unsatisfactory answers to questions about how best to handle the data, both during collection and once the pandemic has subsided. In fact, a poll from the *Washington Post* and the University of Maryland demonstrate the American

---

[5] Morning Consult National Tracking Poll (June 20-22, 2019), available at https://www.uschamber.com/sites/default/files/190645_topline_adults_v2_jb.pdf.

[6] Digital Health Consumer Adoption Report 2019, available at https://rockhealth.com/reports/digital-health-consumer-adoption-report-2019/.

[7] 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/.

[8] 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.

[9] "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.

public's deep privacy concerns about using tech-enabled COVID-19 tracking and tracing systems that could help limit the pandemic's deadly toll.[10] The lack of reliable assurances of how entities will collect, use, and exchange data has fostered reticence from the public to use technologies like public health contact tracing apps.

Finally, HHS' recently finalized interoperability and information blocking rules are poised to drastically impact the exchange, access, and use of electronic medical records. While the AMA wholeheartedly supports the intent of the rules to make it easier for patients to access their electronic health information, the rules lack safeguards to help ensure that patients understand what they are consenting to when they grant permission to an app to access their medical records. The AMA advocated strongly and regularly for HHS to include controls in the final rule to promote transparency on how apps use health information, whom apps share health information with, and how patients could prevent the apps from profiteering off of their data. Unfortunately, HHS failed to take meaningful action in its final rule to promote this type of transparency. As a result, patients may be less willing to share information with physicians for fear that technology companies and data brokers will have full authority over the use of their indelible health data.

The AMA believes that mobile health apps and associated devices, trackers, and sensors must abide by applicable laws addressing the privacy and security of patients' medical information. The AMA encourages the mobile app industry and other relevant stakeholders to conduct industry-wide outreach and provide necessary educational materials to patients to promote increased awareness of the varying levels of privacy and security of their information and data afforded by mobile health apps, and how their information and data can potentially be collected and used. **The FTC has a valuable opportunity to help foster public trust by strengthening its rules for how apps may use and disclose patient's health information and should, at a minimum, expand the HBN Rule's coverage to specifically include direct-to-consumer technologies and services such as mobile health applications (apps), virtual assistants, and platforms' health tools** (collectively referred to as "entities" in this letter).

The FTC Should Redefine "Unauthorized Access" To Promote Individuals' Understanding of Data Collection and Sharing Practices

Section 13407 of the American Recovery and Reinvestment Act of 2009 (Recovery Act),[11] which is the basis for the HBN Rule, and the HBN Rule regulations require PHRs to report the acquisition of unsecured PHR identifiable health information without the authorization of an individual. This definition highlights a pressing question in contemporary discussions around privacy: whether individuals truly understand what information they are authorizing a PHR (or other entity) to acquire, use, and share, simply by clicking "accept" through a series of terms and conditions. Society is increasingly recognizing that a consumer cannot truly, properly authorize the exchange of information without clearly knowing who is receiving the information. The moment a consumer installs an app, it begins searching for that person's data. Even the most vigilant consumer may unwittingly install an app mining for their personal information as nearly every app comes packaged with a range of Software Development Kits (SDKs). As companies have abused SDKs to siphon up personal user data even when they are not supposed to, SDKs

[10] Timberg, C. et al. "Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic." *The Washington Post*. April 29, 2020. Available at https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/.

[11] Public Law 111-5, 123 Stat. 115 (2009).

have evolved as loopholes in our privacy. Accordingly, we strongly urge the FTC to redefine the term "unauthorized access" as described below to inject greater transparency into the PHR and related-entities ecosystem by incorporating the following recommendations in its HBN Rule.

The FTC should define "unauthorized access" as presumed when entities fail to disclose to individuals how they access, use, process, and disclose their data and for how long data are retained. Specifically, an entity should disclose to individuals exactly what data elements it is collecting and the purpose for their collection. Such information should not be used for a materially different purpose than those disclosed in the notice at the point of collection of such information. For example, an entity that collects location data to provide weather should not use that data for advertising. Entities should only collect the minimum amount of information needed for a particular purpose, in accordance with regulation and/or federal guidance. For example, a weather app may need general location data (e.g., zip code), but not precise location data (e.g., GPS coordinates). Entities should also make public their data retention policy stipulating which data will be used and for how long. For example, an entity should disclose a policy stating which data elements are retained for operational or regulatory compliance needs. The policy should also explain who is responsible for each category of data and that data are disposed of if no longer needed. Absent this level of specificity, individuals are not truly providing entities with authorized data access.

Furthermore, the FTC should define "unauthorized access" as presumed when an entity fails to disclose to an individual the specific secondary recipients of the individual's data. The *Wall Street Journal* has reported on 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.[12] 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.[13]

---

[12] Sam Schechner and Mark Secada, Wall Street Journal, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.* (Feb. 22, 2019), available at https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[13] 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.

Social media companies are not the only recipients of this information; 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.[14]

Lastly, **the FTC should clarify that "unauthorized access" will be presumed if an entity's privacy policy is not written to promote understanding by those with elementary school levels of reading comprehension.** There is an alarming 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 describing how his or her data will be used. An 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."[15] These facts reveal a significant failing in fundamental concepts of equity. Rather than permitting this industry practice to continue, the FTC should require entities to use clearly defined and unambiguous terms in their privacy policies. For example, statements such as, "We may share this data with our partners to improve quality" are vague and should not be permitted. Rather, clear and specific statements such as, "We will share your name, date of birth, and lab results with your employer because you have signed up for their workplace wellness program" should be promoted.

The FTC should Require Entities to Make Their De-Identification Processes and Techniques Publicly Available

The FTC asks whether the definition of "PHR identifiable health information" should be modified in light of technological advances in methods of de-identification and re-identification. Rather than opining on the most appropriate method of de-identification, we first note that there is disagreement among stakeholders over whether information can ever be truly de-identified.[16] Additionally, some data historically not considered "personal" or "identifying" (e.g., IP addresses, advertising identifiers from mobile phones) may in fact be both. For example, 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

[14] 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.

[15] 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.

[16] Erin Brodwin, STAT, *Google research suggests efforts to anonymize patient data aren't foolproof* (Feb. 25, 2020), available at https://www.statnews.com/2020/02/25/google-anonymizing-patient-data-an-uphill-battle/.

geographic location as he or she moves through various apps.[17] This 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."[18] As National Public Radio and ProPublica report, "it isn't hard to understand the appeal of all of this data to insurers:"

> 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…allow[ing] insurers to deny coverage to sick patients.[19]

Accordingly, we urge the FTC to require greater accountability and transparency from entities claiming that they have deidentified an individual's PHR health information. Specifically, **the FTC should revise the definitions section of its HBN Rule to clarify that entities must make their de-identification processes and techniques publicly available.**

Decrease the Threshold for Immediate Reporting to the FTC

The FTC notes in its request for comment that the FTC's website lists only two breaches of the HBN Rule, "because the Commission has predominantly received notices about breaches affecting fewer than 500 individuals."[20] **The AMA believes that the public may be better served by the HBN Rule if it requires public reporting of breaches affecting fewer than 500 individuals.** Strengthening the FTC's enforcement activity in this way would lead to an increased level of transparency and more accurate reporting of those individuals whose information has been improperly disclosed. Accordingly, the AMA urges the FTC to provide additional information to the public regarding the notices it received that impacted fewer than 500 individuals. For example, if the FTC received numerous notices that impacted 300-499 individuals perhaps the 500+ standard should be revised to require reporting for breaches impacting 300 or more individuals. Again, this emphasis on increased transparency would help to build confidence in the use of technologies such as mobile health apps and encourage the public to regard the FTC as a reliable resource to consult when evaluating which platforms they should entrust with their health data.

In conclusion, the AMA believes that the FTC should continue to serve as the nation's leading consumer protection agency and use its authority to bring enforcement actions against any non-covered HIPAA entity that seeks to intentionally undermine the consumer's trust by sharing information, be it health or other pertinent personal data, without consumer knowledge. The AMA believes that the FTC's review of the HBN Rule is significant in light of the dramatic surge in consumer use of cloud based PHRs and other technologies that assist individuals in managing their health conditions and we appreciate the opportunity

---

[17] 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.

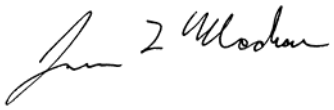
[18] Kaitlyn Tiffany, Vox Media Network, *Angry Birds and the end of privacy* (May 13, 2019), available at https://www.vox.com/explainers/2019/5/7/18273355/angry-birds-phone-games-data-collection-candy-crush.

[19] 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.

[20] 85 Federal Register 31085.

to provide these comments. If you have questions, please contact Laura Hoffman, Assistant Director, Federal Affairs at laura.hoffman@ama-assn.org or 202-789-7414.

Sincerely,



James L. Madara, MD