AMERICAN PSYCHIATRIC ASSOCIATION

800 Maine Avenue, S.W.
Suite 900
Washington, D.C. 20024

August 2, 2023

Chair Lina M. Khan
U.S. Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
Attn: Division of Privacy and Identity Protection, Bureau of Consumer Protection

Re: Health Breach Notification Rule, Project No. P205405

Dear Commissioner Khan:

The American Psychiatric Association (APA), the national medical society representing over 38,000 psychiatric physicians and their patients, appreciates the opportunity to comment on the proposed rule to modify the Health Breach Notification (HBN) Rule to increase consumer health data protections. This is a critical starting point in establishing accountability and transparency for protection of health-related data by non-HIPAA-covered entities.

APA is supportive of enhancing the definition of "health care services or supplies" to "include any online service … that provides health-related services or tools," including mobile applications that host "wellness" data, like sleep, fitness, or diet information. Data that can indicate the presence of mental illness can be derived from many non-HIPAA-protected sources, including search terms, social media use, and consumer behavior, and can be combined with data from other generative sources to produce highly granular, individually-identifiable information. APA supports efforts to increase the privacy and security of all such data.

The availability of mobile health applications is a crucial tool in supporting access to and the quality of health care services, helping mitigate a severe shortage of mental health and other clinicians through patient self-help, symptom monitoring, and information. Confidentiality is critical to ensuring that patients access needed mental health care services. **If these technologies are not private or secure, users that are the most vulnerable – including those without in-person care options, those with lower digital literacy, and those with significant mental health needs – are at the greatest risk of harm to their privacy and well-being.**[1, 2] Online services can offer an appealing, theoretically discreet, alternative to those that fear stigma from their communities for seeking help, and failures in protecting these users can risk

[1] Psychological Data Breach Harms.
[2] On the privacy of mental health apps.

enhancing existing avoidant behavior, paranoia, or discomfort as well as put users actively in harm's way (e.g., due to exposure to harmful algorithms or "dark patterns"). In fact, **APA's App Evaluation Model identifies the privacy and security of an app as the foundational step in evaluating the appropriateness of using technology in clinical settings.**[3]

To enhance the protections proposed by this rule, we urge FTC to expand the definition of what constitutes user consent to privacy policies. It is well-established that most users do not read privacy policies, and privacy policies are text-heavy, long documents, often written in "legalese," that most users do not fully understand.[4] To mitigate deceptive use of data, companies that are regulated by the FTC should be required to:

- Make language in privacy policies accessible to users, ideally at no more than a sixth-grade reading level.
- Present key information in large print with fewer words, with each key element requiring affirmative agreement.
- Present the risks associated with agreeing to the privacy policy.

To help consumers better understand the arrangements and risks associated with their user data, FTC could consider creating a rating scale as a framework for communicating with consumers the risk of different types of data use arrangements as outlined in company privacy policies (e.g., red = company policies allow them to sell all user data, yellow = company has rules in place about what other companies can do with the data sold to them, green = company does not sell or otherwise transfer your data to third parties). **Efforts at transparency and consumer education also may generate momentum toward enhanced data protection policies by affected companies.**

FTC acknowledges implicitly in this draft rule that many consumers may erroneously assume that their health-related data are protected by HIPAA and, consequently, may not understand that much of their consumer online behavior that indicates their health status is unprotected. **In addition to enhancing system-level user protections, APA recommends that FTC can undertake a public awareness campaign, with the help of expert stakeholders, to help users understand where their data are unprotected and what actions they can take to protect their privacy.**

Recognizing certain limitations on FTC's ability to enforce upstream data protections, **APA urges FTC to apply its authority to define unfair or deceptive practices and issue the Commercial Surveillance and Data Security Proposed Rule to establish a framework enabling FTC to regulate data privacy and security protections *before a breach occurs*.** Given the ever-increasing rate of exposure to privacy and security risks due to increasing access to online tools, increasing sophistication of data aggregation and person-level matching capabilities, and the increased potential for profit associated with unrestricted access to data, FTC's enforcement role must grow alongside the market for consumer data.

[3] The App Evaluation Model: Privacy.
[4] Americans' attitudes and experiences with privacy policies and laws.

The FTC's Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking noted that, "As networked devices and online services become essential to navigating daily life, consumers may have little choice but to accept the terms that firms offer."[5] **Breach notifications are not an adequate consumer protection strategy in instances where consumers do not have viable alternatives to allowing a company use of their data.** In HIPAA-covered health care settings, if a patient does not want their data shared beyond the walls of a practice for non-health care delivery purposes (e.g., for research or with a health information exchange), the patient's opt-out does not preclude them from receiving care. In consumer settings, if a customer does not want their health-related data shared or sold, their only alternative is to not be a customer of the company. In situations where the customer does not have an alternative – consider a smaller town with one big box store where purchases are associated with the customer's credit card, or a large online marketplace that offers the lowest-priced options for many health-related consumer goods – customers are left with the option to either not buy the products they need *or* protect the privacy of their health-related data. The FTC should explore ways to protect the consumer from this unwinnable situation by identifying applicable enforcement authorities to protect consumer data in advance of a data breach.

APA is supportive of FTC's efforts to expand health-related data protections and urges FTC to explore additional ways to protect consumers. **We offer the support of psychiatrists with expertise in informatics, in partnership with FTC, to develop policies and education around online protection of people with mental illness.**

Thank you for your review and consideration of these comments. If you have any questions or would like to discuss any of these comments further, please contact Abby Worthen (aworthen@psych.org), Deputy Director, Digital Health.

Sincerely,

Saul M. Levin, M.D., M.P.A., FRCP-E, FRCPsych
CEO and Medical Director
American Psychiatric Association

[5] Trade Regulation Rule on Commercial Surveillance and Data Security.