AMERICAN
PSYCHIATRIC
ASSOCIATION

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

September 28, 2023

The Honorable Bill Cassidy, M.D.
Ranking Member, HELP Committee
U.S. Senate
Washington, DC 20510

Dear Senator Cassidy,

The American Psychiatric Association (APA), the national medical specialty society representing over 38,000 psychiatric physicians and their patients, appreciates the opportunity to provide comment on health data protection strategies. APA appreciates the timeliness of issuing this RFI and shares your commitment to improving health outcomes through data and technology while protecting privacy. Regulatory frameworks governing health data sharing and data protection have taken on new importance in recent years, and online protection of people with mental health and substance use disorders merits specific consideration.

Given the existing administrative burdens facing clinicians, and that technology typically develops faster than regulation, the roles of the agencies and stakeholders in protecting patient data should be fully explored before revising HIPAA. For example, issuance of the Federal Trade Commission's (FTC) pending Commercial Surveillance and Data Security Proposed Rule would advance efforts to establish a framework enabling FTC to regulate consumer health data privacy and security protections. The Substance Abuse and Mental Health Services Administration's (SAMHSA) recent draft rule proposing to reform substance use disorder data protections under 42 CFR Part II and the Office of the National Coordinator for Health IT's (ONC) recent draft Health Data, Technology, and Interoperability rule are pending frameworks working toward protection of sensitive or patient-requested data beyond HIPAA. Simultaneously, the health care workforce and affordability crises necessitate support and reduction in administrative burdens for clinicians, requiring partnership to establish technical assistance and incentives for health care entities to understand their legal obligations and uptake appropriate, high-quality technology in their practices.

As noted in the RFI, health information is increasingly held by non-health care entities, including mobile applications that host "wellness" data, like sleep, fitness, diet, and location 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 using AI-driven technologies to produce highly granular, individually-identifiable information. 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.

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 and symptom monitoring. 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 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). 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]

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), 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 – 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.

Consumer protections of health-related data require changes to the definition of 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 host health-related data 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.

APA looks forward to collaboration on this critical topic. If you have any questions regarding our comments, or if APA can serve as a resource on these issues to the Committee in its policy development, please contact Mikael Troubh (mtroubh@psych.org), Director, Federal Relations.

Sincerely,

Saul Levin MD, MPA

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

[1] Psychological Data Breach Harms.
[2] On the privacy of mental health apps.
[3] The App Evaluation Model: Privacy.
[4] Americans' attitudes and experiences with privacy policies and laws.