AMERICAN ACADEMY OF FAMILY PHYSICIANS

August 1, 2023

Lina M. Khan
Chair
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

April Tabor
Office of the Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW
Suite CC 5610 (Annex C)
Washington, DC 20580

Re: Health Breach Notification Rule, Project No. P205405

Dear Chair Khan and Secretary Tabor:

On behalf of the American Academy of Family Physicians (AAFP) which represents 129,600 physicians and medical students nationally, I write in response to the Federal Trade Commission's (FTC) notice of proposed rulemaking (NPRM) to amend the Health Breach Notification Rule (HBNR). The AAFP supports the goal of the NPRM and appreciates the FTC taking this step to clarify for organizations not covered by the Health Insurance Portability and Accountability Act (HIPAA) exactly how they are required to notify customers, the Commission, and, in some cases, the media if there's a breach of unsecured, individually identifiable health information.

Among other recommendations detailed below, the AAFP urges FTC to:

- Finalize proposed changes seeking to clarify that mobile health applications are covered by the HBNR and to more explicitly define their obligations under the Rule.
- Finalize the proposed clarification that developers of wellness products (including fitness, sleep, and diet-related) are required to adhere to the Rule, just as app developers of medical products (including medication and disease-related) must.
- Finalize the proposed revision of "PHR related entity" to clarify that any entity offering health products or services through any internet-connected mechanism is a PHR related entity, including mobile health applications, instead of the term only applying to websites.
- Finalize proposed changes to authorize expanded use of electronic means, including email, text messaging, within-application messaging, and electronic banners to notify patients of a security breach.

The AAFP has long supported policies that guarantee the appropriate security of protected health information while working to improve patients' access to their data, as well as the ability to share patients' health information across the care team. We are strongly supportive of making data reliably interoperable while maintaining patient confidentiality, and we acknowledge that ensuring health data privacy long-term is going to require a federal citizen data privacy law and regulatory framework. One way to make health information more accessible and actionable for patients is to enable patients to access their health information through third party applications that they can download to a smartphone or similar device. The AAFP has supported efforts to improve this type of accessibility but

1133 CONNECTICUT AVE., N.W., STE. 1100 | WASHINGTON, DC 20036-4305 | (800) 794-7481 | (202) 232-9033

remains particularly concerned about the privacy, security, use, and transfer of patient and consumer health data in the ecosystem outside of HIPAA, where it is largely unprotected by federal laws or regulations. The AAFP believes federal legislation is necessary to achieve a greater degree of data standardization and adherence to agreed-upon principles related to the privacy of health data. However, we strongly support FTC using its available authority to improve protections in the interim.

Confidentiality and privacy are foundational elements of the patient-physician relationship and particularly important in family medicine, where longitudinal relationships are common. Only in a setting of trust can a patient share the private feelings and personal history that enable the physician to comprehend fully, diagnose logically, and treat properly. While clinicians and health care organizations must follow the HIPAA Privacy Rule, which guards against disclosures of protected health information (PHI), other entities and data that do not qualify as PHI are not bound by the same rules. For example, a "personal health record" (PHR) is an electronic health record that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for a patient. This is separate from a physician or hospital's electronic health record (EHR) system, which is required to follow the HIPAA Privacy Rule and primarily controlled by the health system.

Congress recognized that PHR vendors and PHR related entities—companies that offer services related to, access information in, or send information to PHRs—were collecting consumers' health information but were not subject to the privacy and security requirements of HIPAA. Large technology companies and vendors of PHRs could obtain and inappropriately use extremely detailed information about individuals, including internet search histories, communications, finances, and location data. These companies may also require the surveillance of personal information as a condition of use for apps individuals use to access their health data or improve their health. The FTC's authority to police "unfair and deceptive" practices is key to preventing vendors and data brokers from inappropriately using PHR identifiable health information, and the AAFP appreciates the agency's prior acknowledgment that makers of health apps, connected devices, and similar products must comply with the HBNR.

Clarification of Entities Covered

The AAFP strongly supports proposed changes seeking to clarify that mobile health applications are covered by the HBNR and to more explicitly define their obligations under the Rule. The FTC proposes to revise the definition of "PHR identifiable information" to clarify it applies to traditional health information, health information gleaned from patients' use of apps or online services, and emergent health data inferred from non-health-related interactions. The AAFP supports this proposal and believes it appropriately clarifies the scope of the data covered.

The Commission proposes a new definition for the term "health care provider" that would align with the definition in the Social Security Act and would encompass any provider of health services, including entities furnishing health care services or supplies. While the AAFP appreciates the FTC using the definition of "health care provider" to clearly apply HBNR regulations to a broad range of stakeholders, including technology vendors, we remain concerned that federal agencies use a variety of definitions for key terms like "health care provider." Disparate definitions for the same terms across different health IT and other health care regulations can create confusion and administrative burdens for physician practices working to ensure they are in compliance. We urge the FTC to align the terms and definitions used in rulemaking with other health IT regulations. Additionally, we urge the Commission to clarify in the final rule, as well as in related educational materials and sub-regulatory guidance, that the safe harbor protections related to "Treatment, Payment, and Health Care Operations" (TPO) in the HIPAA Privacy Rule will not be impacted by these definitional differences or

by any other revisions made to the HBNR. This clarification is important to minimize confusion for physician practices and ensure care is not disrupted.

The FTC's newly proposed definition of "health care services or supplies" would include any website, mobile application, or internet-connected device that permits tracking a variety of health-related data, including medications, diseases, vital signs, fertility, and fitness. The AAFP appreciates the clarity provided in this proposed definition and supports the Commission's goal of ensuring developers of health apps and similar technologies understand their notice obligations under the HBNR. **We strongly support the FTC's clarification that developers of wellness products (including fitness, sleep, and diet-related) are required to adhere to the Rule, just as app developers of medical products (including medication and disease-related) must**.

Clarification Regarding Types of Breaches Subject to the Rule

The AAFP supports the proposal to expand the definition of "breach of security" by adding a sentence to clarify that a breach is not limited to cybersecurity or nefarious intrusions, but instead includes any disclosure of PHR identifiable health information that was not authorized by the patient. A voluntary disclosure made by a PHR vendor that wasn't authorized by the patient can be just as damaging as an unauthorized disclosure from a data breach, and we appreciate the Commission's action to iterate that clearly.

Revised Scope of PHR Related Entity

The FTC proposes revising the definition of "PHR related entity" to clarify that any entity offering health products or services through any internet-connected mechanism is a PHR related entity, instead of the term only applying to websites. **The AAFP strongly supports this revision, as many patients access their health information through mobile applications and deserve the same level of security and privacy as those utilizing websites for the same purpose**. The AAFP acknowledges the potential for overlap between a PHR related entity and a third party service provider, and we support the FTC's proposed revision to clarify when a third party service provider would not be considered a PHR related entity.

Clarification of What it Means for a PHR to Draw Information from Multiple Sources

The FTC proposes to amend the statutory definition of a "personal health record" to clarify that a product that can draw information from multiple sources is a personal health record even if a patient limits the information drawn to one source. The Commission also proposes to clarify that if a product can draw any information from multiple sources, it is a personal health record even if it only draws health information from a single source.

The AAFP supports these proposed amendments because it would help ensure patients' data remains protected and secure, regardless of which limits an individual patient chooses for an app. We believe these changes would clarify for vendors which of their products are subject to the HBNR and thus would encourage vendors to maintain compliance.

Facilitating Greater Opportunity for Electronic Notice

The AAFP strongly supports the Commission's proposals to authorize expanded use of electronic means, including email, to notify patients of a security breach. The Rule currently permits notice by postal mail and only permits the use of email in limited circumstances. The FTC proposes that written notices could be sent by either postal mail or email, provided the individual specified email as their preferred primary contact method. Further, the Commission proposes defining electronic mail to "email in combination with...text message, within-application messaging, or electronic banner". We strongly agree with the FTC's conclusion that these proposals will align the HBNR's communication methods with how most individuals receive similar breach notices, and we

appreciate the proposed structure of providing notice in two different electronic formats to increase the likelihood individuals will see them.

Expanded Content of Notice

The Commission proposed several changes to expand the content of the security breach notice, including a brief description of potential harm; full contact information for any third parties that acquired unsecured PHR identifiable health information; a description of the types of unsecured PHR identifiable health information involved; a brief description of what the breached entity is doing to protect impacted individuals; and an expansion of the communication methods provided to individuals with which they can contact the breached entity and discuss resolutions.

The AAFP supports patients having full access to data and details about their health and health care, particularly if their personal health information has been compromised in any way. Patients must have confidence in who is handling their data. Vendors and developers that are trusted with an individual's PHR identifiable health information should be required to provide as much context, clarity, and detail as possible to patients impacted by a security breach. **We support these proposals being finalized and thank the FTC for their leadership in protecting patients**.

In conclusion, the AAFP appreciates the FTC's efforts to preserve and protect the privacy and security of a patient's health information by amending the HBNR to provide greater clarity for all stakeholders. We support the majority of these proposals and appreciate the opportunity to comment. The AAFP is grateful for the FTC's continued efforts and leadership in protecting patients' health data and privacy. Please contact Mandi Neff, Regulatory and Policy Strategist, at 202-655-4928 or mneff2@aafp.org with any questions or concerns.

Sincerely,

Sterling Ransone, Jr., MD, FAAFP
American Academy of Family Physicians, Board Chair