



Physicians Caring for Texans

August 8, 2023

Lina M. Khan, Chair  
Federal Trade Commission  
Office of the Secretary  
600 Pennsylvania Ave. NW, Suite CC-5610  
Washington, D.C. 20580

Submitted via [Federal Register](#)

Dear Chair Khan,

On behalf of the Texas Medical Association (TMA) and our more than 57,000 physician and medical student members, thank you for the opportunity to comment on the [Health Breach Notification proposed rule](#) posted to the *Federal Register* on June 9, 2023. TMA appreciates that the Federal Trade Commission (FTC) is strengthening the privacy and security protections for information contained in electronic personal health records (PHRs) when the entities holding the information are not subject to the privacy and security requirements of HIPAA.

For years, TMA has taken a keen interest in PHRs and has made numerous recommendations regarding them to the Centers for Medicare & Medicaid Services and to the Office of the National Coordinator.

TMA believes that individuals should be empowered to address their own health needs and should have mechanisms such as apps to compile their information from disparate sources into one easy-to-navigate location. TMA policy supports the concept that patients should be able to use their PHR as a source of information regarding their medical status. Patients should be able to access their health information conveniently via their PHR and control how that information is shared. Additionally, patients should have assurances from PHR application providers that the information is safe and only shared as the patient directs. For this reason, TMA appreciates the position FTC is taking in the aforementioned proposed rule.

**TMA offers the following overarching comments.**

TMA recognizes that patients access information via mobile technology more often than through any other medium. The complexities of the terms of services created by application providers make them difficult for the average lay person to understand. For this reason, TMA recommends that FTC and other government agencies support industry efforts to develop standardized terms of service that are easy for patients to understand and that include strong privacy provisions. FTC should require application

providers to adhere to these privacy provisions, and patients should be able to rely on the provisions as acceptable.

TMA has adopted the following policy on personal health records that may help inform FTC as it finalizes its proposal:

1. TMA supports the use of personal health records (PHRs) by individuals and families.
2. TMA supports the concept that patients should be able to use their PHR as a source of information regarding their medical status.
3. PHRs need standardized formats that contain at minimum core medical information necessary to treat the patient.
4. TMA supports legislative efforts directed at providing incentives to facilitate PHR use and maintenance.
5. Physicians should be able to access PHR-released information free of charge.
6. TMA supports interoperability of PHRs allowing access to patient health information in patient-care settings.

### **TMA offers the following comments specific to FTC’s proposed revisions.**

#### Clarification of Entities Covered

FTC proposes to revise several definitions in order to clarify the rule and better explain its application to health apps and similar technologies not covered by HIPAA. The proposed rule would modify the definition of “PHR identifiable health information” and adds two new definitions, for the terms (1) “health care provider,” and (2) “health care services or supplies.” The definition of health care provider in this regulation is proposed to mean a provider of services as defined in 42 U.S.C. 1395x(u), a provider of medical or other health services as defined in 42 U.S.C. 1395x(s), or any other entity furnishing health care services or supplies. The term health care services or supplies is proposed to include any online service, such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, or diet, or that provides other health-related services or tools.

#### *TMA Response*

TMA agrees with FTC’s intended clarification of what constitutes a PHR. TMA has strong concerns, however, with the new definition for the term “health care provider.” This new definition is intended to clarify that developers and purveyors of health applications and internet-connected devices, such as fitness trackers, that are not covered by HIPAA are covered by this proposed regulation; however, as drafted, this new definition will have unintended consequences.

The current HHS definition of “health care provider” focuses on those providing what is commonly understood to constitute medical care or health care. Expanding the definition of “health care provider”

as proposed by FTC to encompass others, e.g., calorie counters, will create unnecessary confusion among consumers. TMA, therefore, strongly recommends that FTC delete the definition of “health care provider” and instead clarify that for purposes of the PHR identifiable health information definition, the information must have been created or received by a HIPAA-covered entity (while adding in employers and the new non-HIPAA covered entities desired to be included by FTC).

#### Clarification Regarding Types of Breaches Subject to the Rule

FTC proposes to revise the definition of “breach of security” to clarify that a breach of security includes an unauthorized acquisition of PHR identifiable health information in a personal health record that occurs as a result of a data security breach or an unauthorized disclosure.

#### *TMA Response*

TMA agrees with FTC’s proposal, as it makes clear that incidents of unauthorized access trigger notification obligations and are not limited to cybersecurity intrusions or other nefarious behavior.

#### Revised Scope of PHR-Related Entity

FTC proposes to revise the definition of “PHR related entity” in two ways. First, FTC is proposing language to clarify that PHR-related entities include entities offering products and services not only through the websites of vendors of PHRs but also through any online service, including mobile applications. Second, FTC proposes to revise the definition of PHR-related entity to clarify that it applies to entities that access or send *unsecured PHR identifiable health information* to a personal health record – rather than entities that access or send *any* information to a personal health record.

#### *TMA Response*

TMA agrees that the second definition revision captures the intent of FTC by narrowing the scope of which entities are subject to the breach notification requirements defined in this proposed regulation.

FTC specifically sought comment about a scenario describing a third-party service provider such as an analytics firm that receives PHR identifiable health information and then sells that information without the consumer’s authorization. FTC believes this would be a reportable breach. TMA agrees with FTC’s assessment. Third-party firms as described should have a compliance obligation just as the PHR-related entities and should be required to notify the vendor of personal health records or the PHR-related entity of a breach. This is similar to how HIPAA business associates are treated under HIPAA breach notification rules (wherein they have obligations to notify the HIPAA-covered entity) if a breach occurs at or by the business associate. TMA further agrees that data could be scrubbed to remove patient-identifying information, and that data could be used for analytics and research.

FTC also seeks input on how to distinguish between the PHR-related entity and a third-party service provider. TMA agrees there should be a way to distinguish between the two types of entities.

#### Clarification of What It Means for a Personal Health Record to Draw Information From Multiple Sources

FTC proposes revising the PHR definition to mean “an electronic record of PHR identifiable health information on an individual that has the technical capacity to draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual.”

*TMA Response*

TMA agrees with FTC's proposed PHR definition revision that clarifies that PHRs include applications with the technical capacity to draw information from multiple sources, regardless of the patient's preference to activate the technical capability.

Expanding Use of Electronic Means for Breach Notifications


FTC proposes to authorize use of email and other electronic means of providing clear and effective notice of a breach to consumers. Currently, regulations require that notices be sent by either postal mail or, in limited circumstances, email.

*TMA Response*

TMA understands that since the regulation is focused on patients and consumers agreeing to use electronic tools for their PHR, it makes sense to provide notices electronically. TMA cautions that in cases where an email is returned undeliverable, the PHR-related entity should resort to postal mail. In line with FTC's desire to provide a clear and conspicuous message, FTC should consider requiring a subject line that starts with "Breach of Your Health Information" so that attention is appropriately drawn to the importance of the message content. This should apply to email and in-app notifications regardless of whether the PHR-related entity uses the model notice or not.

TMA appreciates the opportunity to provide feedback on the [Health Breach Notification proposed rule](#). Any questions may be directed to Shannon Vogel, associate vice president of health information technology, by emailing [shannon.vogel@texmed.org](mailto:shannon.vogel@texmed.org) or calling (512) 370-1411.

Sincerely,



Rick W. Snyder II, MD  
President  
Texas Medical Association