Comments of Consumer Reports
In Response to the
Federal Trade Commission
Notice of Proposed Rulemaking on the
Health Breach Notification Rule

By

Matt Schwartz, Policy Analyst
Justin Brookman, Director of Technology Policy

August 8, 2023

Consumer Reports appreciates the opportunity to provide feedback on the Federal Trade Commission's (FTC) Request for Comment on its Notice of Proposed Rulemaking on the Health Breach Notification Rule (HBNR). We thank the Commission for initiating this proceeding and for its other efforts to rein in excessive commercial data practices.

We view this rulemaking as essential, as many companies that collect especially sensitive personal information, including health-related data, fail to safeguard it with the appropriate care. The FTC's recent enforcement actions in this area reveal a concerning trend of companies with access to personal health information improperly sharing it with third-parties or otherwise breaking their privacy promises to consumers.[1] Similarly, a 2021 Consumer Reports investigation into seven of the leading mental health apps showed that they had significant privacy issues: many shared user and device information with social media companies and all had confusing privacy policies that few consumers would understand.[2] Stricter requirements guiding how companies may collect and share consumers' health information are long overdue.

Below, we respond to each of the questions posted in the Request for Comment, describing our views on the proposed updates to the Health Breach Notification Rule in detail.

Analysis of Proposed Changes

1. Clarification of Entities Covered

The Commission proposes clarifying that the term "PHR identifiable information" means information:

> (1) that is provided by or on behalf of the individual;
> (2) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual;

---

[1] See, e.g., Federal Trade Commission, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others, (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google; Federal Trade Commission, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order, (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc; Federal Trade Commission, FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising, (March 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook; Federal Trade Commission, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising, (February 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising

[2] Thomas Germain, Mental Health Apps Aren't All As Private As You May Think, Consumer Reports, (March 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/

(3) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and
(4) is created or received by a health care provider, health plan, employer, or health care clearinghouse.[3]

In general, we support clarifying the definition to encompass data that meets these conditions. The proposed definition is already included in the current rule by cross-reference, so it should not take any stakeholders by surprise. The definition also largely aligns with modern definitions of "health information" and "consumer health information" in state privacy laws with similar aims in attempting to eliminate the HIPAA coverage gap. For example, Washington's recently passed My Health, My Data Act defines "consumer health information" as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."[4]

At the same time, we suggest several improvements that would expand the coverage of the definition. First, we believe the Commission should define PHR identifiable information as any information that is collected *about* the individual, rather than just information provided by or on behalf of the individual. Some information collected by health-related apps may include information that arguably was not directly provided by the consumer (device configuration information that a company collects without the consumer's input) or on behalf of the consumer (for example, most data sent to advertisers). We believe the Commission has the authority to adopt this formulation, as the Recovery Act simply says PHR identifiable information "includes" information provided by or on behalf of the individual;[5] the Commission could reasonably interpret the definition to include more types of information than are included in the statute.

On the second prong of the definition, we ask that the Commission clarify that device level information collected from individuals counts as PHR identifiable information. As the Commission is aware, tracking in the mobile ecosystem is often carried out through the use of advertising or device identifiers, which persistently follow a device user as they browse the web or apps. While such identifiers may or may not be immediately associated with an individual's full name, identification can be accomplished when device identifiers are linked with certain common, highly specific data elements, such as one's real-time location data.[6]

---

[3] Federal Trade Commission, Notice of Proposed Rulemaking, Health Breach Notification Rule, Proposed Section 318.2(i), (June 9, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule#footnote-81-p37830

[4] My Health My Data Act, Section 3(8)(a), https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Session%20Laws/House/1155-S.SL.pdf?q=20230803083054

[5] American Recovery and Reinvestment Act of 2009, Section 13407 (f)(2)(a). https://www.congress.gov/bill/111th-congress/house-bill/1/text

[6] See, e.g., de Montjoye, YA., Hidalgo, C., Verleysen, M. et al., Unique in the Crowd: The privacy bounds of human mobility, Sci Rep 3, 1376, (March 2013), https://doi.org/10.1038/srep01376, (concluding that just a four random location data points are uniquely identifiable 95% of the time).

The Commission notes that it believes its definition would cover inferences companies generate about individuals' health from non-health-related data points (presumably because the definition includes data "created" by a healthcare provider).[7] While such inferences are created by using data initially provided by the consumer, consumers often have very little transparency into how their data is subsequently used to generate assumptions about them, let alone an ability to correct such data if it is inaccurate. If disclosed, business' assumptions about consumers' health status carry the risk for personal embarrassment, social stigmatization, discrimination, could be used as a basis to make legal or other similarly significant decisions, or create other harms. Consumers should be notified when this information is shared without their authorization. We support the Commission's interpretation on this point and note that derived health information is included in Washington's new health privacy law.[8]

The Commission also proposes a definition for a new term, "healthcare provider", which includes entities that furnish "health care services or supplies".[9] Together, these new definitions would ensure that apps that provide healthcare related functions, such as mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet and treatment, are required to provide breach notices when they share PHR identifiable data with unauthorized recipients.

We think both changes are appropriate, as they align with the statutory intention that entities that are not covered entities under HIPAA but that access information in a personal health record or send information to a personal health record provide breach notices. These changes reflect the growing ecosystem of entities that can access, collect, or share health-related information, as well as the growing suite of healthcare related functions these players can provide. Currently, many of these entities exist in a gray area where, due to the sensitivity of the services they offer, consumers think they must meet special legal protections, when, usually, no such protections exist. In a 2023 study headed by University of Pennsylvania researchers, 82% of consumers didn't realize that HIPAA does not apply to many health-related data in mobile apps.[10] As a result, many consumers share their information with these businesses under false pretenses.

Many of these companies explicitly market themselves as providing important health care services while at the same time sharing information with advertisers and big tech companies.[11]

---

[7] Federal Trade Commission, Notice of Proposed Rulemaking, Health Breach Notification Rule, Proposed Section 318.2(i)(4), (June 9, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule#footnote-81-p37830

[8] My Health My Data Act, Section 3(8)(b)(xiii), https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Session%20Laws/House/1155-S.SL.pdf?q=20230803083054

[9] Id., Proposed Sections (e)-(f).

[10] Turow, J., Lelkes, Y., Draper, N. A., & Waldman, A. E, Americans Can't Consent To Companies' Use Of Their Data, (February 20, 2023), https://repository.upenn.edu/asc_papers/830/

[11] Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, "'Out Of Control': Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies," The Markup, (December 13, 2022),

The new definitions of healthcare services or supplies and health care provider modernize the Rule to reflect the current reality that consumers regularly use apps to manage their care, alongside websites and other technologies, not currently obligated to provide enhanced privacy protections. As healthcare within these modalities grows in popularity, consumers, at a minimum, should receive the same protections as are required of traditional healthcare providers.

2. Clarification Regarding Types of Breaches Subject to the Rule

Recent Commission HBNR enforcement actions center around the interpretation that the personal information within personal health records can be breached when vendors and related entities *voluntarily* share PHR identifiable information.[12] To further solidify this, the Commission proposes updating the Rule by adding a sentence at the end of the current definition of "breach of security" stating that: "[a] breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach or an unauthorized disclosure."[13]

We agree that the proposed change is necessary and sufficiently clarifies for the marketplace the Rule's coverage. It is important to note that the Recovery Act frames breaches of security in relation to individuals, rather than to vendors of personal health records or PHR related entities. The proposed change is consistent with the plain language of the current Rule and the Recovery Act's definition of "breach of security", since that term simply means "acquisition of such information without the authorization *of the individual* (emphasis added)."[14] For this reason, the Rule should cover breaches where a vendor of personal health records or a PHR related entity *voluntarily* shared the individual's PHR identifiable health information without the individual's authorization, as well as breaches where a regulated entity did not intend to share the information. We share our view on what should constitute consumer "authorization" below.

Despite the statute's clarity, due to the Commission's longstanding (until recently) non-enforcement of the Rule, this understanding of "breach of security" might not be immediately intuitive to businesses. This further supports the Commission's reasoning in codifying the change in the Rule.

3. Revised Scope of PHR Related Entity

---

https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies

[12] See *supra,* note 1.

[13] Federal Trade Commission, Notice of Proposed Rulemaking, Health Breach Notification Rule, Proposed Section 318.2(a), (June 9, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule#footnote-81-p37830

[14] American Recovery and Reinvestment Act of 2009, Section 13407(f)(11), https://www.congress.gov/bill/111th-congress/house-bill/1/text

The Commission proposes revising the definition of PHR related entity to include any entity that offers products or services through the website or online service of a vendor of personal health records. We support this revision for the reasons articulated in the Notice of Proposed Rulemaking — health records are increasingly accessed via mobile applications and other non-website technologies, so PHR related entities should include those that provide services to such entities.

The Commission also proposes limiting the definition of PHR related entity to only include entities that access or send *unsecured* PHR identifiable health information (rather than any type of information) to a personal health record. Accordingly, entities that access or send *secured* PHR identifiable health information would not be responsible for notifying individuals when a breach has occurred. According to Department of Health and Human Services Guidance, information is deemed secured when it has been encrypted as specified in the HIPAA Security Rule or when it is destroyed.[15] This is a reasonable standard, as the disclosure of fully encrypted information without a decryption key would not pose a substantial privacy risk to individuals (assuming the data is encrypted both in-transit and at rest) and would be of very little value to attackers or other possible purchasing entities, such as data brokers. This is also a similar standard to that of many existing state privacy laws, which tend to exempt from coverage any information that has been "de-identified" (which often means information that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person), provided that the controller or other recipients promise not to attempt to re-identify it.[16]

Finally, Consumer Reports agrees that third parties should be responsible for notifying vendors of personal health records or PHR related entities — rather than notifying the consumer directly — when they have disclosed PHR identifiable information without authorization. Vendors of personal health records or PHR related entities should carry the ultimate responsibility of notifying consumers when the consumers' health information has been the subject of a breach or unauthorized sharing — whether that breach occurred on their part or because of an action by one of their third-party contractors. Otherwise, consumers may be confused by receiving notifications from entities that they do not have a direct business relationship with.

4. Clarification of What it Means for a Personal Health Record To Draw Information From Multiple Sources

The Commission proposes revising the definition of personal health record so that an electronic record of PHR identifiable information qualifies so long as it has the *technical capacity* to draw information from multiple sources, even if it does not actively draw information from multiple sources.

---

[15] Department of Health and Human Services, Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

[16] See, e.g., Virginia Consumer Data Protection Act, Section 59.1-581, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

Consumer Reports supports this change and notes that the Commission is burdened by the Recovery Act's outdated understanding of personal health records.[17] The justification for personal health records being defined as those that pull information from multiple sources seems to stem from a time when traditional healthcare institutions dominated the market for healthcare technology and data. Lawmakers likely envisaged personal health records as platforms where patients could upload lab results, ask questions, and share information with their traditional healthcare provider.

However, as previously noted, the market has changed. Consumers now upload and share health information similar to that of which was previously imagined with a variety of specialized apps and services in order to manage their care. In many cases, healthcare providers have no relationship with these apps and services, even as consumers share extremely granular and personalized types of data with them. Though it is undoubtable that these apps and services constitute extensive records of an individual's health, those that only pull information from a single source would not be covered by the Rule. This lack of statutory foresight leaves consumers severely underprotected and is a confusing construct to understand; most consumers would find it extremely objectionable if their personal health information was shared with third-parties without their authorization, regardless of the underlying app or service's technical ability to draw information from more than one source.

Therefore, the Commission's solution to interpret personal health records as those that can pull *any* type of information from multiple sources (instead of just health information) is likely the best way to expand the reach of the rule while still hewing to the limitations of the statute. The Commission should also interpret the existence of any API capable of importing data from a third-party, coupled with the consumer's ability to input their own data, as satisfying the criteria. This will help ensure inclusion of certain healthcare related apps that otherwise meet the Rule's coverage thresholds and that present an inherently higher risk for data breaches due to the potential for technical misconfigurations or other problems in transferring the data.

In addition, the Commission should also consider how information *submitted* from a single source (i.e. the consumer) may in fact be *drawn* from information collected from several disparate sources. For example, a consumer filling out a health questionnaire on an app may reference formal lab results and input a resting heart rate collected from a wearable, even if the wearable is not capable of being linked to the app. This interpretation would expand the reach of the Rule even further to encompass more apps and services that otherwise behave like personal health records.

5. Facilitating Greater Opportunity for Electronic Notice

The Commission proposes clarifying that the methods of sharing breach notices include written notice through email if the individual has specified electronic mail as the primary method of communication. The Commission also proposes defining email to mean email in combination

[17] American Recovery and Reinvestment Act of 2009, Section 13400(11), https://www.congress.gov/bill/111th-congress/house-bill/1/text

with text messages, in-app messaging, or electronic banners. The Commission notes that it prefers this two part notification so that businesses cannot choose the electronic method of communication less likely to be seen by consumers. We support updates to the Rule that allow consumers to receive notifications via email if they wish. However, Consumer Reports is concerned that the two-part structure may require consumers to share more information than they desire (i.e. their email address) when they wish to only receive notification via text messages, in-app messaging, or electronic banners. Consumers that want to receive notifications through any of the non-email modalities should be able to do so without surrendering unnecessary information. The Recovery Act provides legal justification for allowing this type of notification; Section 13402 (e)(1)(b) states that when a business has "insufficient" contact information to provide written notification, it may provide a "substitute form of notice." We urge the Commission to interpret text messages, in-app messaging, or electronic banners as a substitute form of notice for consumers that do not wish to share a mailing or email address.

We also support mandating use of standardized notice designs (allowing businesses to substitute the specific circumstances of a given breach) proposed by the Commission. Model notices have the advantage of creating uniformity in communications to consumers and will prevent businesses from attempting to confuse or mislead consumers as to the nature of or responsibility for the breach.

6. Expanded Content of Notice

The Commission is proposing five changes to the content requirements for breach notifications.

1. *A brief description of the potential harm that may result from the breach*. We agree that this element is important, as it will allow consumers to begin taking steps to mitigate the harms from a breach (for example, by being more vigilant about suspicious activity on unrelated accounts if identity theft is cited as a potential harm). While we recognize that there are limits to the usefulness of this type of information, especially when a business does not yet understand the full extent of the breach, it still may benefit consumers in certain circumstances.
2. *Full name and contact info of third-party that has acquired unauthorized data, if known.* We agree that disclosing the identity of the breaching entity to consumers is crucial to help them understand the severity of the breach. This information can be highly relevant to consumers as they take steps to protect themselves or decide whether to trust the company in the future. The identity of the unauthorized third-party may be more objectionable or have the potential to cause disproportionate harm to certain groups compared to others. For example, some consumers may take particular interest when their information has been shared with a social media company or an entity with a given political orientation.
3. *A description of the types of information involved in the breac*h. As healthcare providers collect evermore sophisticated types of personal health information, it becomes harder for the average consumer to understand how their data is being used. For example,

some companies collect sophisticated health inferences that might not be obvious to most consumers. Other companies may collect extremely granular tracking data about a consumers' usage of an app. A description of these types of data compromised in a breach will provide more clarity to consumers about the nature of the harm than a broad category of information would.

4. *A description of how the breached entity is protecting affected individuals in the wake of the breach.* Requiring that breached entities share this information will incentivize them to take proactive measures to mitigate harms to consumers, instead of just communicating what they are doing to prevent future breaches. This information will be relevant to consumers' future decisions to continue their relationship with a given business after a breach.
5. *Two or more contact procedures*. The current Rule allows breached entities to provide to consumers contact methods that do not align with modern communication practices. Such methods (i.e. requiring that consumers send a letter via postal mail) could likely depress consumers' ability to ask questions and receive timely information about a breach. Companies, at the least, should be required to allow consumers to ask questions by email or by phone. We support the proposed update.

7. Proposed Changes To Improve Rule's Readability

Consumer Reports supports the proposed changes made to improve the Rule's readability.

Changes Considered but Not Proposed and on Which the Commission Seeks Public Comment

1. Defining Authorization and Affirmative Express Consent

The current definition of "breach of security" means the acquisition of unsecured PHR identifiable information without the "authorization" of the individual. "Authorization" is not currently defined in the Recovery Act, existing Rule, or proposed Rule, and the Commission requests comment regarding the tradeoffs between defining the term or relying on existing commentary and Commission settlements to provide guidance.

As a general matter, Consumer Reports does not believe that the concepts of "authorization" or "affirmative express consent" are best suited to protect consumer privacy interests in today's world. Consumers' privacy should be protected by default through strong data minimization provisions — companies should be prevented from collecting or sharing any information they do not need to provide the service. We elaborate on these principles in our Model Privacy Bill.[18] Applying this understanding to the HBNR, any data sharing not necessary to provide the service would constitute a breach worthy of notice to consumers.

[18] Consumer Reports, Model State Privacy Act, Section 103, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf

However, given that a consent-based framework is encoded into the underlying statute through the authorization requirement, we recognize that the Commission likely cannot justify data minimization requirements in this Rule.[19] Therefore, Consumer Reports agrees with the spirit of the commentary in the current Rule, which says that consumers need to provide "meaningful choice" in authorizing sharing and notes that "buried disclosures in lengthy privacy policies" do not meet this standard.[20]

However, we believe that defining "authorization" directly in the Rule would set a clearer standard for businesses to follow and disincentivize gamesmanship on the part of businesses to exploit gray areas. For example, while the Commission's commentary in the current Rule states that "the Commission *expects* [emphasis added] that vendors of personal health records and PHR related entities would limit the sharing of consumers' information" beyond certain uses implied to be authorized, it is unclear whether this has the same legal effect as *requiring* that those entities limit such sharing.[21]

The Commission should borrow from existing health privacy laws, such as Washington's recently passed My Health, My Data Act, which create a strong standard for consent (the Commission could simply substitute "consent" with "authorization"):

> *"Consent" means a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement, which may include written consent provided by electronic means.*
>
> *(b) "Consent" may not be obtained by:*
>
> *(i) A consumer's acceptance of a general or broad terms of use agreement or a similar document that contains descriptions of personal data processing along with other unrelated information;*
> *(ii) A consumer hovering over, muting, pausing, or closing a given piece of content; or*
> *(iii) A consumer's agreement obtained through the use of deceptive designs.*[22]

This standard makes it clear that the hypothetical examples provided by the Commission would likely not count as consent. Authorization could not be obtained through a "pre-checked" box, because that would not constitute a clear affirmative act. Authorization could not be obtained when a consumer is not required to review terms and conditions because this would not

---

[19] Notably, "Breach of Security" means "acquisition of such information without the authorization of the individual," American Recovery and Reinvestment Act of 2009, Section 13407(f)(11), https://www.congress.gov/bill/111th-congress/house-bill/1/text

[20] Federal Trade Commission, Final Rule, Health Breach Notification Rule, Section 318.2: Definitions (a) Breach of security, (August 25, 2009), https://www.federalregister.gov/documents/2009/08/25/E9-20142/health-breach-notification-rule

[21] Id.

[22] My Health My Data Act, Section 3(6)(a-b), https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Session%20Laws/House/1155-S.SL.pdf?q=20230727132139

constitute “informed” consent (though we do question the degree to which everyday consumers can ever provide truly informed consent to extensive and technically sophisticated data collection and sharing practices). Authorization through a general privacy notice would also not constitute a “specific” agreement —companies would be required to provide a stand-alone request to share consumer data.

2. Modifying Definition of Third Party Service Provider

The Commission has retained the current definition of “third party service providers” but asks for feedback on whether the term appropriately covers current business practices, which commonly include the provision of analytics and advertising services. We believe that it does. Under the plain text of the current rule, any entity that provides services to a personal health record or PHR related entity and “[a]ccesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses PHR identifiable health information” is a third party service provider.[23] So long as the Commission defines PHR identifiable health information to include device or advertising identifiers, most analytics providers and advertisers would trigger the definition of third-party service provider.

3. Changing Timing Requirements

The Commission seeks comment on the current timing requirements for when a breached entity must notify consumers and the Commission. Under the current Rule, entities must notify consumers within 60 days of a breach[24] and the Commission within 10 days of a breach.[25] We believe that these requirements strike an appropriate balance between providing consumers actionable information about a breach, while requiring that breached entities disclose their breach as quickly as possible to the Commission so it can investigate further. However, one possible alternative would be to require that breached entities also notify consumers within 10 days of a breach, but allow regulated entities to provide the more detailed notification that satisfies the content requirements in Section 318.6 after 60 days. That way, consumers may take steps to protect themselves immediately while they await more detailed information about the extent of the breach.

****

We thank the Federal Trade Commision for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwartz (matt.schwartz@consumer.org) or Justin Brookman (justin.brookman@consumer.org) for more information.

---

[23] Federal Trade Commission, Final Rule, Health Breach Notification Rule, Section 318.2(h)(2), (August 25, 2009), https://www.federalregister.gov/documents/2009/08/25/E9-20142/health-breach-notification-rule

[24] Id., Section 318.4(a)

[25] Id., Section 318.5(c)