U.S. PIRG

Before the
FEDERAL TRADE COMMISSION
Washington, DC 20554

Proposed Amendments to the Health Breach Notification Rule
16 CFR part 318, Project No. P205405

Comments of

U.S. Public Interest Research Group (PIRG)

August 8, 2023

Filed by:
R.J. Cross (rj@pirg.org)
Patricia Kelmar (pkelmar@pirg.org)
And
Ed Mierzwinski (edm@pirg.org)

U.S. PIRG

The U.S. Public Interest Research Group (PIRG) is writing in response to the FTC's proposed rulemaking to amend the Health Breach Notification Rule. Our brief comments are followed by **9,659 petition signatures from PIRG members and the general public asking the FTC to finalize strong rules that better protect health data in the digital age.**

U.S. PIRG broadly supports the Commission's proposed changes and is encouraged to see the agency continuing its efforts to modernize the consumer protections under the Commission's jurisdiction and address the technological changes shaping today's markets and consumers' experiences. Since its creation, the Health Breach Notification Rule has been underutilized, and is an appropriate tool for reining in unchecked harmful data practices.

U.S. PIRG is a public interest research and advocacy organization. Since our founding in the 1970s, we've worked to uncover threats to public health and well-being and fight to end them, using the time-tested tools of investigative research, grassroots organizing, advocacy and litigation. U.S. PIRG's mission is to deliver persistent, results-oriented advocacy that protects consumers, encourages a fair, sustainable economy and fosters responsive democratic government.

Our Don't Sell My Data campaign in particular works to protect consumers from the harmful impacts of corporate data practices. In our data protection work, U.S. PIRG has previously filed comments with the Commission regarding its ANPR on commercial surveillance and data security, and submitted more than 7,100 petition signatures supporting a petition for rulemaking to prohibit the use on children of design features that maximize for engagement.

U.S. PIRG would like to offer the following support and suggestions pertaining to the Health Breach Notification Rule. U.S. PIRG would also like to express support for the comments filed by the Electronic Privacy Information Center (EPIC).

1. **Expanding the definition of entities covered.**

U.S. PIRG supports the new and modified definitions of the Health Breach Notification Rule expanding the scope of covered entities to include websites, mobile applications and other digital devices like smartwatches capable of gathering and connecting consumer health data.

In the last decade, the industry of digital and data-driven health services has grown immensely. Virtually all of the devices and apps gathering and aggregating identifiable health information outside doctor's offices and hospitals fall outside of HIPAA's jurisdiction. Given the changes in the marketplace and technologies, it's appropriate for the FTC to ensure any tools gathering identifiable medical information are regulated to protect consumer privacy.

U.S. PIRG

It's appropriate for the scope of the Rule to apply to entities or to the type of information entities may process. Many companies gather and monetize health information; any entity engaged in these processes must be accountable for their data practices, regardless if they brand themselves as a health-related company or not.

Data brokers & health AdTech companies

The Commission should ensure that data brokers are included in this rule. Many data brokers aggregate health signals about consumers, pulling from sources such as app usage, web searches and purchase histories, and using these disparate data points to create lists and profiles of individuals. These data broker operations can collect significant amounts of data focused on health. For example, the data broker and AdTech firm Tremor offers over 400 "standard health segments that are available and may be used by Tremor International group companies' clients to deliver targeted advertising".[1] These segments include those with "major health issues", "neurodevelopment disabilities" and "memory loss", as well as those who are "vape users" or have an "opioid interest."

Health-specific advertising technology companies should also be on the FTC's radar as companies that aggregate health information. For instance, the health AdTech company DeepIntent offers a Patient Planner service - "the only tool that unifies medical and pharmacy claims" according to its website.[2] Its Outcomes platform "links real-world clinical data with impression data" and provides access to "third-party segments onboarded from industry-leading data providers".[3] Another firm that may be instructive to examine is PulsePoint, another health advertising technology company, that is owned by the same parent company as WedMD and receives data from WebMD and its other related health sites and apps.[4]

2. **Clarifying the definition of "breach of security".**

U.S. PIRG supports the clarification of the definition of "breach of security" and its inclusion of the unauthorized acquisition of identifiable health information resulting from an unauthorized disclosure. Unauthorized disclosures to technology companies and advertisers require regulatory oversight, and the use of the Health Breach Notification Rule in this capacity is appropriate. Consumers currently have few meaningful protections against excessive data collection and the unwarranted sharing, selling and monetization of sensitive information.

U.S. PIRG supports EPIC's point that a breach of security ought to include an entity that collects more identifiable health information than necessary to serve the purpose for which it was

---

[1] Tremor, "International Health Segments List", archived on August 8, 2023 at: http://web.archive.org/web/20230808171901/https://www.tremorvideo.com/wp-content/uploads/2020/08/Tremor-International-Health-Segments-List.pdf. Tremor has 4 offices in the United States - Los Angeles, New York, Chicago and Bellevue, WA.

[2] See "Patient Planner" on https://www.deepintent.com/planners/. Accessed on August 8, 2023.

[3] DeepIntent case study "Prescriptions Over Impressions", available for download at https://www.deepintent.com/cs-prescriptions-over-impressions/. Accessed on August 8, 2023.

[4] https://www.pulsepoint.com/

collected. The more data companies collect, the more likely it is that sensitive information will be exposed in a breach in a hack.

The Commission's proposed changes to the Health Breach Notification Rule are an important step towards protecting consumers in today's digital economy. U.S. PIRG looks forward to continuing to work with the Commission to curb the rampant data collection and monetization practices that have been significantly under-regulated to date and put consumers in harm's way unnecessarily.

Petition

Below is the petition language signed by 9,659 PIRG members and members of the general public to the FTC regarding the Health Breach Notification Rule NPRM.

> *Re: Document ID FTC-2023-0037-0001*
>
> *Doctor's offices and hospitals aren't allowed to share our medical records with companies — and neither should online tools. But right now, health apps and websites are permitted to share our personally identifiable medical data with companies like Google and Facebook, who in turn use that private information to target us with ads — all without notifying us that our data was used this way.*
>
> *I strongly support the proposed rule requiring all apps and websites collecting health information to notify the FTC and affected individuals of any unauthorized disclosure of personally identifiable health data — including sharing with tech companies and advertisers.*

Signers begin on the next page. To protect the privacy of signers, only first name, last initial and city are provided.