
**Comments of the World Privacy Forum to the Federal Trade Commission regarding Health Breach Notification Rule, Project No. P205405**

*Sent via regulations.gov*

Federal Trade Commission,
Office of the Secretary,
600 Pennsylvania Avenue NW,
Suite CC–5610 (Annex H),
Washington, DC 20580.

8 August, 2023

The World Privacy Forum welcomes the opportunity to comment on the Commission's Notice of Proposed Rulemaking, Health Breach Notification Rule, 88 Federal Register 37819 (June 9, 2023), https://www.federalregister.gov/d/2023-12148.

The World Privacy Forum (WPF) is a nonprofit, non-partisan 5011(c)(3) public interest research group. WPF focuses on multiple aspects of privacy, with health privacy being among our key areas of work. We publish a large body of health privacy information, including guides to HIPAA; reports and FAQs for victims of medical identity theft; and materials on genetic privacy, precision medicine, electronic health records, and more.[1] We testify before Congress and federal agencies, and we regularly submit comments on health privacy regulations. WPF is the co-chair of the World Health Organization's Research, Academia, and Technical Constituency, (co-chairing with the CDC.) WPF also serves on a data governance workgroup at WHO. You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and comments at http://www.worldprivacyforum.org.

[1] See World Privacy Forum, *A Patient's Guide to HIPAA,* https://www.worldprivacyforum.org/2019/03/hipaa/. See also our Health Category page for additional materials at https://www.worldprivacyforum.org/ category/health-privacy/.

## I. Introduction and background to the comments

In 2009, WPF commented on the first FTC data breach NPRM.[2] The initial proposed rules were narrow, and our comments sought to broaden them where possible and appropriate. In 2021, WPF, noting that the Health Breach Rule had not been enforced yet, urged that the Commission apply the breach regulations to an enforcement action where the Rule may have potentially been applied.[3] The Commission declined to apply the health breach notification rule in this particular case, however, in the past year, however, the Commission has begun to take a broader view of its remit in the commercial health breach area and has in fact now begun enforcing the Health Breach Rule.

Specifically, we recognize that the Commission has taken some actions to enforce its rules against *deception* in this area.[4] We do not disagree with these actions. However, those actions do not establish any meaningful standards for *unfairness*, and that is where the need is greatest. It bears repeating that not all of the limitations of the Breach Rule are wholly the responsibility of the Commission, as the Congress bears much of the responsibility for its limits on Commission activities. We note the narrow language that Congress provided to the FTC regarding a Health Breach Rule. This is the context in which we offer these comments. We do not expect the Commission to cure all ills in this rulemaking. We also see the wisdom in not attempting to do so.

## II. Discussion

### A. The fundamental challenge the unregulated health data ecosystem poses

We write these comments against an exceptionally difficult backdrop. With this NPRM, we fully acknowledge the Commission's good intentions. We must also acknowledge the difficult reality that even at its best, the proposal is only able to address a small aspect of the current consumer non-HIPAA health data universe. This limitation has in part been imposed on the FTC by the narrowness of Congress' original language regarding the rule. This limitation also exists because of the extraordinarily messy boundaries of the unregulated health data and health-related data ecosystem in the US, another issue that the FTC does not have meaningful control over.

---

[2] Comments of World Privacy Forum to the Federal Trade Commission regarding Health Breach Notification Rulemaking, 1 June 2009. https://www.worldprivacyforum.org/wp-content/uploads/2009/08/WPF_FTCBreachcomments_06012009_fs.pdf .

[3] Comments of World Privacy Forum to the Federal Trade Commission regarding Proposed Consent Order, In the Matter of Flo Health, File No. 1923133, March 2021. https://www.worldprivacyforum.org/2021/03/wpf-urges-us-federal-trade-commission-to-re-examine-data-breach-notification-requirements-for-health-data-in-flo-health-proposal/ .

[4] For example, the Commission enforced the rule in the GoodRX Holdings case, https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising . WPF published a brief blog noting the enforcement action. https://www.worldprivacyforum.org/2023/02/ftc-takes-action-against-health-apps/ .

As a result, the Commission's proposal does not approach the fundamental problem that consumer health data (as well as most other consumer data) is essentially unregulated for the protection of consumer privacy. Merchants, websites, cell phone apps, and numerous other entities operating in todays expansive digital ecosystems can collect, compile, analyze, lease, share, and sell consumer data largely without restriction. This is generally true of most data, and it is also specifically true of health-related data that is not specifically regulated by HIPAA.

In some cases, consumers may receive some notice and have some rights, but as we discuss at length in the *Scoring of America*, a 2014 benchmarking report on AI, consumer scoring, data analytics, and consumer data, the American marketing industry (including data brokers) collects, compiles, and monetizes consumer data without effective notice to or involvement of the consumers who are the subjects of the data being sold.[5] This has been true for decades, and it has been exacerbated by newer data analysis techniques that facilitate identity resolution without directly utilizing what most consumer laws consider to be "PII." WPF has testified about data brokers before Congress now multiple times, including in 2011, 2013, 2015, and 2019. Most recently, we submitted comments to the CFPB Request for Information regarding Data Brokers, and provided an extensive overview of the modern data broker ecosystem, and that it will soon become nearly impossible to regulate effectively.[6] In the CFPB comments, we describe more about modern data brokering techniques. Later in these comments, we will return to the definitional challenges and propose some potential solutions.

We mention the consumer data industry here because Congress has not yet taken any meaningful measure to act to solve some of the extensive data-related problems affecting people, households, and groups of people today. All of this is relevant to the Health Breach Notification Rule because this Rule is one of the few regulations applying to the health-related layer of the consumer data ecosystem. Even if this rule can impact a small sliver of the health data ecosystem, it is worth that effort. Because today, health data that is relevant to people's lives and well-being is no longer existing only under the auspices of HIPAA. And that data can pose meaningful risks that are non-theoretical.[7]

---

[5] Pam Dixon and Robert Gellman, *The Scoring of America: How secret consumer scores threaten your privacy and your futur*e, World Privacy Forum, 2014. https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/ .

[6] *Comments of the World Privacy Forum Regarding Request for Information*, Docket No. CFPB-2023-0020, Consumer Financial Protection Bureau, Regulations.gov. https://www.regulations.gov/comment/CFPB-2023-0020-4033 .

[7] *HIPAA and Reproductive Health: A companion FAQ to the Patient's Guide to HIPAA,* World Privacy Forum, July 2022. https://www.worldprivacyforum.org/2022/07/hipaa-and-reproductive-health-a-companion-faq-to-the-patients-guide-to-hipaa/ .

**B. Hobson's Choice: No rulemaking, or a narrow rulemaking that potentially creates different standards**

In our view, this NPRM addresses breaches of some poorly-defined categories of consumer data for some not-very-clearly defined categories of data controllers. We repeat that there is no general substantive rulemaking controlling the processing of consumer data. At best, the current effort is a drop in the bucket as compared to the need.[8] In some ways, a narrow rulemaking may be worse if it means that we end up with many separate standards and rules governing consumer data and maybe different standards and rules for the same type of consumer information depending on who the data controller is and which agency regulates the controller.

While WPF supports and wants rules and especially good rules for consumer data, including health data held outside of HIPAA, we are concerned that a very narrow rulemaking may create considerable consumer confusion and a barrier to change because once a rule is in place for some data controllers, they will surely resist being subject to a broader and more uniform rule. Little of this is the Commission's fault because much of this problem is the result of congressional enactment of piecemeal privacy laws. We propose a solution at the conclusion of the comments.

**C. Breach notices need to have value to the consumer**

We have doubts about the value of breach notices for the class of processors covered by the rule, for several reasons. We know from our experience advising consumers that many consumers learned long ago to disregard most breach notices. Some consumers don't understand the lengthy and legalistic notices, and some don't believe that they can do anything about a breach. The other side here is that some consumers are genuinely concerned about various consequences of data breach and identity theft. In the financial realm, there are effective actions that consumers can take on their own (e.g., credit freezes) to address their concerns. Consumers may be offered free services after a breach, or may purchase (or offered) some form of identity theft monitoring or other services. These services can be assistive in financial sector identity theft monitoring. The difficulty for non-HIPAA health data is that identity monitoring services are often not fully effective in this area due to overall structural problems in non-HIPAA-covered health data.

Unlike the breach of financial or credit information, there are few actions that consumers can take when informed of an unauthorized disclosure of their non-HIPAA-covered health information. What meaningful steps can a consumer take if their fitness information shows up for sale on the dark web? What can a consumer do if their general interest in certain prescription medications or disease-specific support groups ends up in a profile maintained by a marketing company? What can a consumer do if non-HIPAA-covered information regarding reproductive

[8] We agree with the sentiment expressed in the Joint Statement of Commissioner Rohit Chopra and Commissioner Rebecca Kelly Slaughter Concurring in Part, Dissenting in Part, Federal Trade Commission, In the Matter of Flo Health (2021) (Commission File No. 1923133) https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc ("…we would prefer to see substantive limits on firms' ability to collect and monetize our personal information…").

health status or even potential reproductive health status ends up in the hands of law enforcement authorities investigating reproductive health care that has become illegal in some states? We do not know of a commercial breach monitoring service that will solve for these particular problems at this time.[9]

All of this being said, informing individuals about data breaches under HIPAA does have value, because HIPAA gives patients defined rights and clearly regulates HIPAA-covered entities. Medical forms of identity theft are serious, and patients and providers need to know about this in order to clean up health files, among other tasks.[10] Breach notification in this context can and is meaningful, because it allows patients to take action. But commercial data breach notification has limited value when individuals are not able to take clear action with the information. In many circumstances that we foresee at this time, breaches of personal information from non-HIPAA health sources are not likely to increase risks of medical forms of identity theft. Therefore, most of the identity-theft-focused solutions currently available that are oriented to supporting consumers who have received a breach notification will not be effective.

We note that the proposed rule would cover a large number of new "providers" who are not subject to sectoral privacy law such as HIPAA. There are well over 150,000 "health" apps at the Apple App Store, and there could easily be many more new entities subject to the Commission's expanded breach rule. Individuals might be inundated with breach notices that could undermine whatever utility the notices offer, and there may be no solutions for the notices the consumers receive.

**Request: An FTC workshop to explore solutions**

We would be interested to see the FTC explore possibilities of solutions with all stakeholders that would help consumers in this area. What could be done here? Reputation-style monitoring? Removal of the information from the dark web? Removal of the information from the downstream partners and entities which also were given the data? What are the potential options and tools that may be available for mitigation and curing harm? We encourage the FTC to hold a workshop specifically to this point, so that stakeholders can be gathered and new solutions can be constructed. Surely, all of the stakeholders here can work together to do more for consumers impacted by these types of data spills, some of which are now attached to potentially serious consequences.

---

[9] We discuss the data problems associated with reproductive health and how HIPAA interacts with these problems in *HIPAA and Reproductive Health: A companion FAQ to the Patient's Guide to HIPAA,* World Privacy Forum, July 2022. https://www.worldprivacyforum.org/2022/07/hipaa-and-reproductive-health-a-companion-faq-to-the-patients-guide-to-hipaa/ .

[10] For more information about this, see, Pam Dixon and Robert Gellman, *Medical Identity Theft: The information crime that can kill you,* World Privacy Forum, 2006. *HIPAA and Reproductive Health: A companion FAQ to the Patient's Guide to HIPAA,* World Privacy Forum, July 2022. https://www.worldprivacyforum.org/2022/07/hipaa-and-reproductive-health-a-companion-faq-to-the-patients-guide-to-hipaa/ . . See also WPF's Medical ID theft page which includes consumer FAQs and other information.

**Request: That the FTC maintain a public listing of breaches similar to the HHS breach listing and portal**

We are also very interested in the FTC creating a listing of all health data breaches under its rule, similar to what HHS publishes at its breach portal.[11] WPF maintains a data visualization of HHS -reported health data breaches, which has been helpful in understanding trends and in studying data breaches.[12] If the FTC is able to create a similar information repository, it would likely be of long-term value in understanding more about how, when, why, where, and what types of data in this category are being breached. This would help consumers, researchers, policy makers, the business sectors, and enforcers alike.

**D. Definitional challenges**

We believe that the biggest problem for any privacy rule focused on health data is definitional. It is nearly impossible to draw clear lines between health and non-health data without a clearly defined context. HIPAA solved this problem efficiently by defining who is subject to the rule. If you are a HIPAA-covered entity, then *all* information that you maintain about individuals is *protected health data* for purposes of HIPAA. No HIPAA-covered entity has to decide if PHI includes a home address, grocery list, vacation destination, workplace, hobby, location, car color, or any other data element associated with an individual. It is all PHI because everything in the files of a HIPAA covered entity is PHI. That is a clearly defined context.

The NPRM offers three definitions that address the scope of the proposed rule: *PHR identifiable information*, *health care provider*, and *health care services or supplies*.

> As revised, ''PHR identifiable information'' would be defined as 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; (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 (as defined in 42 U.S.C. 1320d(5)), employer, or health care clearinghouse (as defined in 42 U.S.C. 1320d(2)).
>
> The proposed Rule also defines a new term, ''health care provider,'' in a manner similar to the definition of ''health care provider'' found in 42 U.S.C. 1320d(3)

---

[11] *Breach Portal*, US Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf .

[12] Interactive Health Data Breach Visualization Map, World Privacy Forum. https://www.worldprivacyforum.org/2016/09/health-breach-interactive/ .

> (and referenced in 1320d(6)). Specifically, the proposed Rule defines ''health care provider'' 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 proposed Rule adds a new definition for the term ''health care services or supplies'' to include any online service, such as a website, mobile application, or internet-connected device that provides 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, or that provides other health-related services or tools.

These definitions present a host of problems.

The first problem here is that the term *health care provider* in the proposed rule uses the same term as HIPAA. This is certain to create confusion. Is someone a health care provider for HIPAA, for PHR, or arguably for both? A HIPAA health care provider cannot be a PHR health care provider, but any reference to *health care provider* is likely to create uncertainty at times.[13] We suggest that the Commission use different words, perhaps *PHR provider*.

A second issue derives from the fact that identifiable information from a HIPAA-covered entity does not come with a HIPAA tag. If HIPAA PHI is disclosed (by a HIPAA health care provider, by the subject of the information, or by a third party), it may not be clear if the information is PHI. The information would remain PHI in the hands of another HIPAA-covered entity but not in the hands of a third party. Consider an individual who reports to a PHR health care provider that he has Kitchen Sink syndrome. Without more context, it is impossible for the recipient to tell if the information is a diagnosis from a HIPAA health care provider, is something made up by the individual, or relates to health care at all. The individual may have a leaky faucet. The proposed definition of *PHR identifiable information* does not help. Without more context, the status of the information is unclear under the proposed rule. The enormous scope of the definition for *PHR identifiable information* contributes greatly to the problem. Anything can be health information in the right context.

A third issue relates to the requirement that *health care services or supplies* include any online service. This is not at all clear. Exactly what constitutes an online service? Consider a walk-in clinic for sleep disorders (one that is not subject to HIPAA) that operates with paper records but allows its customers to make appointments through a mobile application. Is that clinic an *online service*? What about a farmer's market that sells "healthy" organic vegetables from a wooden roadside stand and that has a website that shows its location and hours? Suppose there is no website but the farmer keeps track of customer interests in a phone app so the farmer can call

---

[13] We observe that the term *health care provider* by itself may have a clear meaning in a particular context, but in the absence of a context, confusion is likely.

customers on the telephone when the vegetables they want are available. Is the farmer subject to the proposed rule? The farmer maintains an *online* service because the cell phone is backed up online and is thus an *internet connected device* that *provides a mechanism to track…diet*. More examples of offline activities with some degree of online presence are easy to imagine.

We humbly suggest that nearly all commercial activities today have some form of online presence. We see the limitation in the definition that the online activity must provide "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, or that provides other health-related services or tools." That limitation, however, is quite broad, and will encompass many if not most types of current records or activities. We repeat our observation about the inability to sharply define health data in the absence of a specific context. A "health-related service or tool" is just as unclear.

It is possible to spin out a large number of examples dancing on the edges of the expansive and unclear definitions proposed. Any record of food purchases tracks *diet* information. We can start with a food service that caters to those with diabetes. The food seller knows a customer's diagnosis, and the record of purchases tracks the customer's diet. Another example is a general supermarket selling a wide variety of foods. If some of those items cater to individuals who are on low-sodium diets, who have specific food allergies, or who make other purchases that reflect or imply dietary restrictions or medical conditions, the supermarket's online ordering and record keeping system will make the supermarket subject to the PHR rule. In another example, imagine a seller of canned tomato soup in regular and low-sodium varieties. A purchase of the low-sodium soup implies a potential dietary restriction that meets the definition. But we suggest that a purchaser of the regular variety of tomato soup also reveals diet information, namely that the purchaser is *not* on a low-sodium diet. That is health information just as much as any other dietary limitation or non-limitation.

Here's another example:

1. A diner at a restaurant orders a salad identified on the menu as gluten-free.
2. A diner at a restaurant asks if a salad on the menu can be prepared gluten-free.
3. A diner at a restaurant says that the diner has celiac disease and then orders a gluten-free meal.
4. A diner at a restaurant receives a menu offering dishes that are gluten-free and dishes that are not gluten-free. The diner orders a dish that is not gluten-free.

There is a coherent argument here that, in each case, the diner disclosed personal health information to the restaurant. Note that the restaurant could take orders online, at tableside by a waiter, at a table through a cell phone ordering system, or through a shared network that provides

broader sharing capacity.[14] Note further that ordering from a regular menu (as opposed to a gluten-free menu) implies that the diner is not gluten-free, itself a different medical status. If the restaurant is a chain that shares its records with other locations or uses a food delivery service that accepts orders for the restaurant (and for other restaurants as well), all of the definitional requirements are met. Every entity has a PHR or arguably has a PHR and would likely require a lawyer to help make the decision.

The limitation in the definition of PHR to a provider "that has the technical capacity to draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual" does not help. Consider entities which sell a variety of products, including health-related products on its own and for third party vendors. Depending on how the entity is structured, the entity itself and the third-party vendors may maintain records on customers, and each entity's systems draw information from each other and perhaps from additional sources. Each of these entities will either be clearly or arguably subject to the rule.

The "technical capacity" standard addressing the mere possibility of drawing information from multiple sources only muddies the waters further. This provision would require an entity with only one source to hire a technical expert to determine if the software or the network in use has the capacity to connect to other sources. It will not matter if the entity expressly organized itself to use only one source because using the wrong software package will subject that entity to the rule. Will an entity that bought a "single source" version of software be subject to the rule anyway because the software offers an upgrade path that include additional capacity? There could be a host of technical distinctions that could be relevant to answering this question.[15]

We observe that the scope of the proposed rule and the inherent uncertainties in the definitions present particular challenges for enforcement of the rule. Imposing a rule with so many problems will make it hard for the Commission to enforce it. Every potential defendant will be able to raise threshold legal challenges to enforcement actions. The Commission would need greatly expanded resources to address both the large number of entities potentially subject to the rule and to investigate whether the rule actually applies to those entities. We wonder what current enforcement activities the Commission would have to drop in order to devote resources to the revised and greatly expanded PHR rule.

---

[14] A food delivery network may not only know what foods were ordered and their health implications, but it may have home addresses and phone numbers in a database used by and for all of the different restaurants that use the delivery services. That sharing may meet the *multiple sources* requirement. The home address may be health information as well. A home address may reveal that an individual lives downwind of a coal-fire electricity generator; in an assisted living facility; or in a surgical rehabilitation unit. We believe that in the absence of a context, even home address may be or imply health information.

[15] An example may clarify. Windows 10 came in both Home and Pro editions. The basic installation of the Home edition included the capability of upgrading to the Pro edition with the payment of an additional fee. The Pro edition software was already installed along with the Home edition. The *technical capacity* to run the Pro edition was present on all computers running Windows 10 Home edition, even if the user did not activate the enhanced operating system. Is that type of software upgrade covered by the "technical capacity" language? What if the upgrade was free and only required the press of a button? Does that distinction matter?

**E. Proposed solutions, including the 80-20 rule**

We want to suggest a different approach to the definitional problems in the rule. The main problem is that the proposed rule seeks to cover every possible entity that might conceivably have health data that could be viewed as a PHR. Trying to cover this universe is simply too difficult. A rule will be more practical and easier to enforce if it is clearer about its application, even if a more narrowly constructed rule might not cover the entire universe. Instead of reaching for 100% of a poorly defined universe, the Commission would be better served by a rule that clearly and cleanly covers 80% of that universe. This type of tradeoff between coverage and clarity is a familiar one in many legislative and regulatory endeavors.

A revised rule should provide a context for judging who is covered. We suggest that the context might be more easily defined by looking at the terms under which a product or service is offered to consumers. ***If an entity promotes its offering as addressing, improving, tracking, or informing matters about a consumer's health, then that entity's offering would be subject to the rule***. Thus, any product or services that tracks or addresses physical activity, blood pressure, heart rate, digestion, strength, genetics, sleep, weight, allergies, pain, and similar characteristics would be subject to a PHR rule.

This approach would look at the way that a product or service is offered and what it proposes to do for consumers. The inquiry would focus on what the product or service says it does rather than any hypothetical data use, possible data transfer, or technical capacity. If a website or app says that it is health related, then it would be covered by the rule. A listing of examples would limit any uncertainty if a data controller did not say "health" in promoting its services.

What this approach would exclude is troublesome edge cases where "health" data is collected as a by-product, but is not used for health purposes. Thus, a supermarket selling a broad variety of foods and that tracks all purchases through a frequent shopper program would not maintain a PHR simply by virtue of recording the purchase of some products that have health implications. The supermarket sells food and does not do so as part of a specific health service to customers. A food delivery service, no matter what information it obtains about the source or nature of a customer's order, would not qualify because it offers delivery, a service unrelated to health. A restaurant that collects information about its gluten-free customers does not offer that service with an intent to affect the health of its customers. That restaurant merely complies with the wishes of its customers by offering a variety of choices. We argue elsewhere in these comments that basic information about individuals – home address, for example – may be health information in some context. But the plumber, landlord, employer, or other entity that serves individuals would never acquire regulated PHR data because they do not expressly offer any health service.

Could this approach allow for evasion? The answer is yes, but it is better to be clear than to be comprehensive. There are a large number of "health" apps available for cell phones that want to

promote themselves as offers a health monitoring or improvement service. They will not succeed by downplaying or avoiding the major attraction of their service. If a few recast their offerings to evade the rule (and retain customers despite being vague), so be it. The Commission is good at addressing deception.

**F. Conclusion**

Thank you again for the opportunity to comment on the proposed rule. We appreciate the Commission's work here, and we hope that some of our suggestions may be useful in revising the rule so that any final rule will be clearer for those covered by it, useful to consumers in a meaningful way, and easier for the Commission to enforce.

We reaffirm our requests that the FTC hold a public workshop with all stakeholders to help devise solutions for consumers who have had their data breached under the new rule, and that the FTC begin to publicly track and provide a roster of breaches that allows for comparability as to size, date, location, type of breach, type of data breached, and so on. This will assist in long-term efforts to improve the ecosystem for consumers.

Respectfully submitted,

Pam Dixon,
Executive Director,
World Privacy Forum