NAI Regulatory Summary and Analysis: Statement of the Federal Trade Commission on Breaches by Health Apps and Other Connected Devices

February 2022

About the NAI

Founded in 2000, the Network Advertising Initiative (NAI) is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for digital advertising in multiple media, including web, mobile, and TV.

Contact

David LeDuc (david@networkadvertising.org)
Vice President, Public Policy, NAI

Anthony Matyjaszewski (anthony@networkadvertising.org)
Vice President, Chief Compliance Officer, NAI

Introduction and Summary

In September 2021, the Federal Trade Commission ("FTC" or "Commission") issued a Policy Statement[1] that is intended to clarify the scope of the FTC's Health Breach Notification Rule ("the Rule")[2]. The purpose of the Rule, finalized in 2009, was to hold non-HIPAA entities accountable in cases of health data breaches by requiring them to notify relevant stakeholders, such as U.S. consumers and the FTC. While this Policy Statement did not amend the Rule or revise the Rule's existing definitions, it signals the FTC's intent to expand enforcement under the Rule, and it interprets the following elements more broadly: (1) covered entities, (2) covered health information, and (3) breach of security, as summarized below.

- First, health apps and connected devices, specifically non-HIPAA entities, are covered under the Rule. While the Policy Statement relies on multiple definitions cross-referenced, and it does not explicitly define health apps, applications that consumers use to "store and process data about anything related to health"[3] are likely covered.
- Second, the scope of covered health information includes not only data collected from device sensors (such as fitness trackers measuring steps and heart rate), but also consumer input data, such as weight and calories, when combined with other data.[4]
- Third, and perhaps most important for the digital advertising industry, a "breach" of covered information includes any sharing or acquisition of covered health information without the individual's specific authorization. To be considered a breach does not require an incident wherein information is stolen or taken from a system without the knowledge or authorization by the covered entity. For example, a health app that shares such information with an ad-tech company without the individuals' prior specific consent is a breach and subject to civil penalties.

The FTC will treat each violation of the Rule as an unfair or deceptive act or practice in violation of a federal regulation; violations of the Rule can be subject to a civil penalty of up to $43,792 per violation.[5]

[1] FTC's Policy Statement on Health Breach Notification Rule, Sept. 2021.
[2] Health Breach Notification Rule, 16 C.F.R. § 318.2 (2022).
[3] "Under it, all applications consumers use to store and process data about anything related to health—e.g., your steps, the food you eat, etc.—are 'health care providers.' So too would be retailers that sell health care supplies, like Neosporin and vitamins." Dissenting Statement of Commissioner Noah Joshua Phillips, at 2.
[4] *Id.* Commissioner Phillips's example of covered information includes consumers' steps as well as the food they eat.
[5] FTC Business Guidance, Complying with FTC's Health Breach Notification Rule.

Detailed Summary & Analysis

While this analysis provides general explanations of certain FTC decisions and federal regulations, it is not legal advice. All NAI members should consult with counsel to determine exactly how the FTC's policy statement applies to their specific business activities.

1. Scope of Entities Covered Under the Rule

Under the Rule finalized in 2009, the entities covered are non-HIPAA entities that are either vendors of Personal Health Record (PHR), PHR-related entities, and third-party service providers. Prior to the Policy Statement, it was an unsettled interpretative issue whether the Rule applies to health apps and devices, as the FTC requested for public comment on it as recently as 2020.[6] The Policy Statement declares that such apps and devices are covered entities because they are health care providers and thus vendors of Personal Health Records (PHR).

- Definition of Vendors of PHR: The Policy Statement concludes that health app developers are vendors of PHR by cross-referencing definitions of several key concepts: PHR, vendors, and health care providers. The Rule defines vendors of PHR as a non-HIPAA covered entity "that offers or maintains a personal health record (PHR)."[7] PHR includes information that is created or received by "health care providers."[8] The Policy Statement states that a health app or connected device is a "health care provider" because it "furnishes health care services or supplies."[9] The Policy Statement also implies that health app developers and devices are vendors of PHR, since they maintain a PHR, which is information received by the respective health apps (who are by definition health care providers).

Additional key definitions, particularly for ad-tech companies, include "PHR Related Entity," and "Third Party Service Provider." In most cases, NAI members and ad-tech companies are likely to fall into one of these categories, working as partners with vendors of PHR. These terms are defined as follows:

[6] Health Breach Notification, Request for Public Comment, 85 Fed. Reg. 31085 (Apr. 22, 2020); *see also* Dissenting Statement of Commissioner Noah Joshua Phillips.
[7] Vendor of personal health records means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record. 16 C.F.R. § 318.2(j).
[8] Section 1171(6) of the Social Security Act (42 U.S.C. § 1320d(6)).
[9] FTC's Policy Statement on Health Breach Notification Rule, Sept. 2021.

- Definition of PHR Related Entity: A business is a PHR related entity if it interacts with a vendor of PHR, either by offering products or services through the vendor's website or by accessing information in a personal health record or sending information to a personal health record.[10] Businesses that are already covered by HIPAA are not PHR related entities.

- Definition of Third Party Service Provider: A third party service provider is a business that offers services involving the use, maintenance, disclosure, or disposal of health information to vendors of PHR or PHR related entities. A business is also a third party service provider if it holds, uses, or discloses unsecured PHR identifiable health information.[11]

2. Scope of Data Covered Under the Rule

While the Policy Statement does not explicitly revise the existing definition of health information, it more broadly interprets the definition of Personal Health Record (PHR) to include not only sensor data collected by a health app or device, but also consumer-input data.

- Definition of Personal Health Record (PHR): The Rule defines Personal Health Record (PHR) as "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[12]

The FTC interprets the phrase "can be drawn from multiple sources" more broadly than before. In their Business Guidance published in 2010 (subsequently updated in January 2022), the FTC stated that entities that only maintain health information directly input by consumers are not covered under the Rule. However, the Policy Statement explicitly states that such entities are now covered if they combine that data with any other source of data. Apps that draw information from multiple sources, "even if the health information comes from one source," are vendors of PHR.[13]

- For example, a blood sugar monitoring app that draws health information from only one source (consumer's input) but also takes non-health information from another source (such as dates from a calendar), is obligated to notify about a breach of security.[14]

The Policy Statement also explicitly states that apps that have the "technical capacity to draw information through an API that enables syncing with a consumer's fitness tracker" are covered

[10] Health Breach Notification Rule, 16 C.F.R. § 318.2(f).
[11] Health Breach Notification Rule, 16 C.F.R. § 318.2(h).
[12] Health Breach Notification Rule, 16 C.F.R. § 318.2(d).
[13] FTC's Policy Statement on Health Breach Notification Rule, Sept. 2021.
[14] FTC's Policy Statement on Health Breach Notification Rule, Sept. 2021.

under the Rule. Therefore, health apps and devices that collect sensor information or collect consumer-input information are covered under the Rule. Although the FTC does not directly expand the definition of health information, the interpretation has the likelihood of expanding the scope of covered entities.

This raises questions as to whether health inferences drawn from non-health-related behavioral information would be covered under the Rule. On the one hand, the purpose of the Policy Statement was to specifically hold health apps and devices accountable for breaches. Therefore, the focus of the FTC does not seem to be on the entities that do not directly handle health information. At the same time, the definition of Personal Health Record (PHR) is quite broad -- broad to the point that the information at issue does not necessarily have to be direct health information. PHR is an electronic record of *PHR identifiable health information*, which is defined in terms of *individually identifiable health information* in the Social Security Act.

- Definition of PHR identifiable health information: it means "individually identifiable health information," as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information: (1) That is provided by or on behalf of the individual; and (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."[15]

- Definition of individually identifiable health information: The term "individually identifiable health information" means any information, including demographic information collected from an individual, that— (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) 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—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[16]

Based on the above definitions, PHR would be (1) any information that "relates to the past, present, or future physical or mental health or condition of an individual" (2) that is reasonably linkable to an individual and (3) drawn from multiple sources. This definition is sufficiently broad that it could cover health inferences drawn from non-health behavioral information, since they "relate" to a health condition of an individual and are drawn from multiple sources. Therefore, while the focus of the Policy Statement is specifically on health apps and devices, it appears possible that the FTC could also bring enforcement actions against ad-tech companies that maintain health inferences drawn about individuals, if shared with other parties without individuals' prior authorization.

[15] Health Breach Notification Rule, 16 C.F.R. § 318.2(e).
[16] Section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)).

3. Scope of "breach" definition under the Rule

The Policy Statement explicitly concludes that a "breach" is "not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule."[17] For example, in its 2022 Guidance, the FTC says that a health app sharing data to an ad-tech company without obtaining prior opt-in consent from a user constitutes a breach for the purposes of the Rule.[18]

One thing to note is that unauthorized access does not constitute a "breach" in so far as the information at hand cannot reasonably identify an individual. For example, "de-identified" information is exempt from the Rule.

- Definition of "de-identified" information: Data is de-identified (1) if there has been a formal, documented analysis by a qualified statistician that the risk of re-identifying the individual associated with such data is "very small," or (2) if specific identifiers about the individual, the individual's relatives, household members, and employers (including names, contact information, birth date, and zip code) are removed, and the covered entity has no actual knowledge that the remaining data could be used to identify the individual.[19]

However, the FTC views device identifiers and advertising identifiers as "reasonably identifiable" to an individual.[20] For example, dissenting opinions by Commissioners Wilson and Phillips stated that based on the new Policy Statement, **Flo Health** would have been liable for violating the Health Breach Notification Rule by sharing device identifier information of its users with companies like Google.[21]

While the scope of enforcement is more easily applied to the practices of first parties who are covered (i.e. health apps and connected devices), rather than third parties (i.e. ad-tech companies and other service providers), breaches that occur at the third-party level, however, could implicate third parties.[22]

What to Know About the Rule's Intersection with the NAI Code Requirements

The effect of the FTC's new interpretation is largely consistent with the NAI's existing requirements in effect since the adoption of our 2020 Code of Conduct ("Code") regarding

[17] FTC's Policy Statement on Health Breach Notification Rule, Sept. 2021.
[18] FTC Business Guidance, Complying with FTC's Health Breach Notification Rule.
[19] 45 C.F.R. § 164.514(b).
[20] FTC Business Guidance, Complying with FTC's Health Breach Notification Rule.
[21] Dissenting Statement of Commissioner Noah Joshua Phillips.
[22] 16 C.F.R. § 318.3(b).

collection and use of sensitive data for advertising and marketing purposes, as well as our Code requirements and guidance more broadly pertaining to sensitive health data.

The NAI has long believed that many types of data can be sensitive, even if they do not fall under current legal and regulatory restrictions. This is why the NAI takes multiple measures to limit the collection and use of data for health-related advertising, including an outright prohibition on healthcare and eligibility uses.

The NAI Code has always required a device user's opt-in consent for collection and use of medical or pharmaceutical records in targeting digital advertising. In this manner, the NAI acts as a backstop to HIPAA, since NAI member companies have not been covered entities, historically. However, the NAI understands that this is only a very small piece of the health privacy puzzle, and that for effective privacy regulation companies must also be restricted in the use of other types of data, including sensor data from devices.

Since 2020, the NAI Code also restricts member companies from using sensor data on users' devices for digital advertising purposes without the user's opt-in consent. Thus, if an NAI member company wanted to leverage the data from a heart-rate sensor, or for that matter any sensor on a device, biometric or otherwise, that member would need to obtain a user's consent for access to the sensor data. Such consent would need to be accompanied by clear disclosures about the proposed uses of the data as well as any downstream sharing. Because these strong restrictions apply regardless of whether an NAI member is a covered entity under HIPAA, they are therefore quite consistent with the effect of the FTC's new Policy Statement, which essentially requires notice and consent for use of this data to be shared with partners for advertising and marketing purposes.

In some ways, however, the NAI Code goes considerably further to protect consumers' health privacy, by also restricting inferences based on web browsing, app use, or digital content viewership that can point to user interest in treatments or medications for a variety of sensitive conditions such as mental health, sexually-transmitted diseases, all types of cancer, pregnancy termination, and as of 2020, children's conditions that cannot be treated with over-the-counter medications, as well as many other specific health conditions.

Considerations Regarding User-Entered Health Data

The FTC's policy statement, and recent settlement with Flo Health[23], also highlight the Commission's focus on a topic that the NAI has not directly opined on in the past: the treatment of user-declared, or manually entered, data into an app on a mobile device, if that data pertains to what the NAI considers a non-sensitive condition, such as cold and flu, or weight-loss. Since this data is not collected through a sensor, it does not fall under the aforementioned restrictions. The Code also provides for requiring a user's Opt-In Consent for digital advertising uses of

[23] Decision and Order, *In re Flo Health, Inc.*, F.T.C. File No. 1923133 (June 17, 2021).

Personal Directory Information, such as calendar, address book, phone/text logs, photo/video data, or similar data created by a user that is stored on or accessed through a device. However, at the time of the development of the 2020 Code, the NAI did not contemplate the broader set of user-entered health data that is now a focus of the FTC. However, we believe the FTC's conclusion is consistent with the spirit of the Code. Now that the FTC has clarified the scope of enforcement around the Health Data Breach Rule, app developers, NAI members and other related businesses would be wise to do a thorough inventory of consumer data sources pertaining to health information broadly.

Key References

1. **Statement of the Commission on Breaches by Health Apps and Other Connected Devices (September 2021):** https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

2. **Guidance, Complying with FTC's Health Breach Notification Rule (January 2022):** https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule

3. **Full Text of the Health Breach Notification Rule (August 2009):** https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318