WORLD **PRIVACY** FORUM

Statement of Pam Dixon, Executive Director, World Privacy Forum to the FTC at its Open Commission Meeting

Regarding WPF request that the FTC provide specific, prominent guidance to non-HIPAA regulated entities regarding the use of the term "HIPAA compliant" and its derivatives in privacy representations

18 January, 2024

Chair Khan and Commissioners, first, thank you for your work regarding the privacy practices of health-related websites. In several recent cases, the FTC has found certain privacy representations of non-HIPAA covered entities to be problematic.

Specifically, the Commission has now unambiguously articulated that if a statement posted on a health-related website uses the term "HIPAA compliant" in a privacy policy or elsewhere, that such a statement may constitute an unfair and or deceptive act or practice, depending on the context and use case. A year ago, I made a statement at the FTC's January 2023 Commission meeting explaining the overarching problems with "HIPAA compliant" representations.[1] The FTC has now taken enforcement actions that address the use of "HIPAA-compliant" terminology. This represents meaningful progress. WPF thanks you for this work.

[1] WPF spoke at the 19 January 2023 FTC Open Commission meeting on the topic of "HIPAA compliant" language. In 2023, just one year's time since WPF made the statement, the FTC has made notable progress in addressing this issue, which is particularly clear in the GoodRx case and the BetterHelp case. See note 3 and 4 below for relevant cases and publications. 2023 WPF Statement to the FTC: Statement of Pam Dixon, 19 January 2023, FTC Open Commission Meeting, Available at: https://www.worldprivacyforum.org/2023/01/statement-of-pam-dixon-at-the-ftc-open-commission-meeting-regarding-consumer-confusion-around-health-privacy-statements-on-websites/ .

We are bringing this issue to your attention again today because even though the FTC has brought clear cases [2] and has mentioned the problems of using the term "HIPAA compliant" in other publications,[3] we are still finding significant numbers of health-related websites that are stating they are "compliant with HIPAA," sometimes prominently.

This comprises a range of websites, including those that are using biometric data to analyze the possible presence of genetically linked conditions.[4] Many consumers are likely to see the term "HIPAA compliant" and mistakenly assume that the business is actually a regulated entity under HIPAA. Meanwhile, some web sites making these statements are utilizing consumer data for marketing purposes.

We are pleased that the Commission is addressing these kinds of behaviors as unacceptable in its recent cases. However, despite the Commission's good efforts, the message has not yet penetrated.

---

[2] The FTC has taken enforcement actions asserting that HIPAA claims may deceive consumers. Key cases include GoodRx, February 2023. See: https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising; and Better Help, July 2023. See: https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter. Additional cases include: Henry Schein, See: https://www.ftc.gov/news-events/news/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled-customers-about-encryption-patient); and SkyMed International, Inc., See: https://www.ftc.gov/news-events/news/press-releases/2020/12/company-provides-travel-emergency-services-settles-ftc-allegations-it-failed-secure-sensitive. Regarding GoodRx, the FTC noted that GoodRx:" …Misrepresented its HIPAA Compliance: GoodRx displayed a seal at the bottom of its telehealth services homepage falsely suggesting to consumers that it complied with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a law that sets forth privacy and information security protections for health data." See: https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising. In the GoodRx complaint, the FTC brought a Count regarding privacy misrepresentation. See Count V, paras 98 - 101. In the BetterHelp FTC complaint, see Section D paras 65 -69 regarding "Respondent's Deceptive HIPAA Seal." See: https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpcomplaintfinal.pdf.

[3] *Collecting, using, or sharing consumer health information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule.* Business Guidance, Federal Trade Commission, Sept 2023. Available at: https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach . From the Guidance: "…as we've noted in other guidance, don't make false or misleading claims that you are 'HIPAA Compliant,' 'HIPAA Secure,' 'HIPAA Certified' or the like." *See also*: Elisa Jillson, *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases.* Business Blog, Federal Trade Commission, July 2023. Available at: https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases . From the article: " 'HIPAA Compliant,' 'HIPAA Secure,' and similar claims may deceive consumers."

[4] For example, this emerging category of health-related web sites may request a photograph of a child or adult, and will then conduct a face recognition technology analysis (and perhaps additional biometric analysis) to match phenotypes to genetically-linked conditions such as Noonan Syndrome, KBG Syndrome, among others, depending on the service.

For this reason, and because we are still seeing a problem, we urge and request the Commission to give specific, prominent guidance to non-covered entities highlighting the use of the term "HIPAA compliant" and its derivatives in privacy representations or elsewhere as an unfair and deceptive act or practice under FTC Act Section 5.

As the Commission knows, HIPAA confers specific legal rights to patients,[5] and the differences between rights conferred to patients under HIPAA-regulated entities and those regulated under the FTC Act Section 5 are non-trivial. This distinction needs to be clearly understood by both businesses and consumers. Again, we note the FTC's good work on this issue; we agree that progress has been made. However, we urge additional clear statements to business to further crystallize the issue beyond any doubt or interpretive question.

Thank you again for your work. We stand ready to assist with additional information.

Respectfully submitted,

Pam Dixon
Executive Director, World Privacy Forum
www.worldprivacyforum.org
info@worldprivacyforum.org

[5] See, for example, a point-by-point discussion of the "Seven rights of HIPAA" in *A Patient's Guide to HIPAA*, World Privacy Forum. First publication, 2009. Most recent update: 2019, with addendum in 2022. Available at: https://www.worldprivacyforum.org/2019/03/hipaa/ . The HIPAA Privacy Rule grants the following rights to patients: A right to a notice of privacy practices, the right to inspect and copy your record, right to request confidential communications, right to request amendment, right to receive an accounting of disclosures, right to complain to the Secretary of HHS, and the right to request restrictions on uses and disclosures.