July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

---

[1] *See, e.g.,* Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.

[2] *See, e.g.,* 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 (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[3] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[4] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users.

Impermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium.

The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (*e.g.,* tracking technology vendors) includes PHI. HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply.[5] This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies.

FTC Act and FTC Health Breach Notification Rule

Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. This is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes. As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app.[6] The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[7] Within the last

[5] *Id.*
[6] *See supra* note 3.
[7] *See* Federal Trade Comm'n, *Statement of the Commission on Breaches by Health Apps and Other Connected Devices* (Sept. 15, 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.

few months, the FTC has issued a series of guidance pieces addressed to entities collecting, using, or disclosing sensitive health information.[8]

OCR and the FTC remain committed to ensuring that consumers' health privacy remains protected with respect to this critical issue. Both agencies are closely watching developments in this area. To the extent you are using the tracking technologies described in this letter on your website or app, we strongly encourage you to review the laws cited in this letter and take actions to protect the privacy and security of individuals' health information.[9]

Sincerely,

/s/

Melanie Fontes Rainer
Director
Office for Civil Rights
U.S. Department of Health and Human Services

/s/

Samuel Levine
Director
Bureau of Consumer Protection
Federal Trade Commission

[8] *See, e.g.*, FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking* (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking; Lesley Fair, *First FTC Health Breach Notification Rule case addresses GoodRx's not-so-good privacy practices* (Feb. 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices; Federal Trade Comm'n and the U.S. Department of Health & Human Services' Office of the National Coordinator for Health Information Technology (ONC), Office for Civil Rights (OCR), and Food and Drug Administration (FDA), *Mobile Health App Interactive Tool* (Dec. 2022), https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool; Kristin Cohen, *Location, health, and other sensitive information: FTC Committed to fully enforcing the law against illegal use and sharing of highly sensitive data* (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[9] In addition to the HIPAA Rules, the FTC Act, and the FTC Health Breach Notification Rule, you may also be subject to other state or federal statutes that prohibit the disclosure of personal health information.