

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN**

JANE DOE 1, and JANE DOE 2, on behalf)	
of themselves and all others similarly)	
situated,)	Case No.
)	
Plaintiffs,)	
)	
vs.)	CLASS ACTION COMPLAINT AND
)	DEMAND FOR JURY TRIAL
WORKIT HEALTH, INC.)	
)	
Defendant.)	
)	
)	
)	
)	

STEVEN D. LIDDLE (P45110)
NICHOLAS A. COULSON (P78001)
MATTHEW Z. ROBB (P81665)
LIDDLE SHEETS COULSON P.C.
975 E. Jefferson Avenue
Detroit, Michigan 48207-3101
(313) 392-0015
sliddle@LSCcounsel.com
ncoulson@LSCcounsel.com
mrobb@LSCcounsel.com

DAVID S. ALMEIDA (PHV forthcoming)
ELENA A. BELOV (PHV forthcoming)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024
david@almeidagroup.com
elena@almeidagroup.com

Attorneys for Plaintiffs and the Putative Class

CLASS ACTION COMPLAINT

Plaintiffs JANE DOE 1 and JANE DOE 2, on behalf of themselves and all others similarly situated (“Class Members”) bring this Class Action Complaint against Defendant Workit Health, Inc. (“Workit” or “Defendant”) and allege, upon personal knowledge as to their own actions, and upon information and belief and the investigation of counsel as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action lawsuit to address Defendant’s illegal and widespread practice of disclosing Plaintiffs’ and Class Members’ confidential and personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “Private Information”) to third parties, including Meta Platforms, Inc. d/b/a Facebook (“Facebook”) and other third parties, without Plaintiffs’ knowledge or consent.

2. Information about a person’s physical and mental health—and a person’s history of disorders relating to substance use in particular—is among the most confidential and sensitive information in our society, and the mishandling of medical information can have extremely serious consequences, including discrimination in the workplace or denial of insurance coverage.¹

3. Simply put, if people do not trust that their medical information will be kept private, they may be less likely to seek medical or substance use treatment, which can lead to more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person’s medical providers is vitally necessary to maintain public trust in the healthcare system as a whole.

¹ See Lindsey Ellefson, Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world, WIRED (Nov. 16, 2022), available at <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last visited May 22, 2023) (“While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it’s even more verboten in addiction treatment, as patients’ medical history can be inherently criminal and stigmatized.”); see also Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022), available at <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited May 22, 2023).

4. The need for data security (and transparency) is particularly acute when it comes to the rapidly expanding world of digital healthcare as, of all the information the average internet user shares online, health data is some of the most valuable and controversial.²

5. Despite professing to value patients' privacy and vowing to protect the confidentiality and security of their private and protected health information, healthcare entities, like Defendant, are collecting, in some instances, "ultra-sensitive personal data" about patients ranging from those seeking information about their reproductive rights and options, those seeking information regarding their addictions, and those seeking mental health counseling.³

6. And, while mobile health options have been celebrated as a way to expand treatment options, the tangible, real-world implications and potential for abuse is staggering:

[T]he sensitive information people share during treatment for substance use disorders could easily impact their employment status, ability to get a home, custody of their children, and even their freedom. Health care providers and lawmakers recognized long ago that the potential threat of losing so much would deter people from getting life-saving help and set up strict laws to protect those who do seek treatment. *Now, experts worry that data collected on*

² Protected and highly sensitive medical information collected by healthcare entities includes many categories from intimate details of an individual's conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. See Molly Osberg & Dhruv Mehrotra, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), available at <https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137> (last visited May 22, 2023).

³ Grace Oldham & Dhruv Mehrotra, Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients, REVEAL (June 15, 2022), available at <https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/> (noting that such "personal data can be used in a number of ways. The centers can deliver targeted advertising, on Facebook or elsewhere, aimed at deterring an individual from getting an abortion. It can be used to build anti-abortion ad campaigns – and spread misinformation about reproductive health – targeted at people with similar demographics and interests. And, in the worst-case scenario now contemplated by privacy experts, that digital trail might even be used as evidence against abortion seekers in states where the procedure is outlawed") (last visited May 22, 2023).

*telehealth sites could bring about the harm [the law] was designed to prevent and more, even inadvertently.*⁴

7. Recognizing these incontrovertible facts and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the United States Department of Health and Human Services (“HHS”) has established “Standards for Privacy of Individually Identifiable Health Information” (also known as the “Privacy Rule”) governing how health care providers must safeguard and protect Private Information.

8. Pursuant to the HIPAA Privacy Rule, *no* health care provider may disclose a person’s PHI to a third party without express written authorization.

9. The HIPAA Privacy Rule sets forth policies to protect all individually identifiable health information that is held or transmitted; these are the eighteen (18) HIPAA Identifiers that are considered personally identifiable information. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual. When personally identifiable information is used in conjunction with one’s physical or mental health or condition, health care or one’s payment for that health care, it becomes PHI.⁵

⁴ <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last visited May 22, 2023).

⁵ The 18 enumerated HIPAA Identifiers are: name; address (all geographic subdivisions smaller than state, including street address, city county, and zip code); all elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age); telephone numbers; fax number; email address; social security number; medical record number; health plan beneficiary number; account number; certificate or license number; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web URL; internet protocol (IP) address; finger or voice print; photographic image *and any other unique identifying number, characteristic, or code that could be used to identify the individual*.

10. Healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, only in a limited way, to perform analysis on data key to operations:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... ***If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.***⁶

11. Simply put, further to the HIPAA Privacy Rule, covered entities such as Defendant are ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third party without express and informed consent.

12. Lest there be any doubt of the illegal nature of Defendant's practice, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, ***disclosures of PHI to tracking technology vendors for marketing purposes,***

⁶ *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>, HHS.GOV (last visited March 21, 2023).

*without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.*⁷

13. Here, Defendant is a telehealth provider of addiction treatment, which virtually advertises and offers services to treat substance use disorders and certain mental health conditions, like anxiety and depression.

14. Defendant controls, maintains, and offers its telehealth addiction and mental health services via its website, <https://www.workithealth.com/> (the "Website"), which Defendant encourages patients to use for program registration, seeking substance abuse and mental health programs and services, condition diagnostics, booking medical appointments, locating and/or identifying physicians and treatment facilities, communicating medical symptoms, signing up for substance use programs and counseling, searching medical conditions and treatment options, and much more.

15. Plaintiffs and Class Members are Users of Defendant's Website.

16. Thousands of Users, like Plaintiffs, have visited Defendant's Website to seek substance abuse and/or mental health care.

17. Because of Defendant's unlawful acts, when Plaintiffs and Class Members used Defendant's Website, communications about their Private Information were surreptitiously and simultaneously disclosed to Facebook and other third parties, without first notifying Plaintiffs and without their prior, informed consent or written authorization.

⁷ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited May 22, 2023) (emphasis added).

18. Plaintiffs and Class Members who visited and used Defendant's Website (collectively the "Users") understandably thought they were communicating confidential Private Information with only trusted healthcare providers.

19. This belief was eminently reasonable because, before Plaintiffs and Class Members provided any information through Defendant's Website, Defendant affirmatively and prominently promised Plaintiffs and Class Members that "All of the information you share is kept private and is protected by our HIPAA-compliant software."⁸

20. After Workit Users, including Plaintiffs, clicked on the "Continue" button to sign up with Defendant, the "Start your Workit profile" page once again assured users that "We take your privacy seriously. Your information is protected by our HIPAA compliant software." Defendant's statement prominently encouraged users to provide personal and admittedly HIPAA-protected information to Defendant prior to signing up, with assurances that any private information they provide will be kept private.⁹

21. However, unbeknownst to Plaintiffs and Class Members, Defendant had embedded an undetectable tracking Meta Pixel (the "Pixel" or "Facebook Pixel") on its Website, which automatically transmits to Facebook every click, keystroke and intimate detail about their Private Information, medical symptoms, conditions and treatments, and disclosed it to Facebook.

22. Also unbeknownst to Plaintiffs and Class Members, Defendant also embedded an undetectable code analytics tool called Google Analytics on its Website, which automatically collected user information and tracked their activities on Defendant's Website, including Plaintiffs' private medical information, and disclosed it to Google.

⁸ <https://app.workithealth.com/signup> (last visited June 27, 2023).

⁹ https://app.workithealth.com/onboarding/zip_code (last visited June 27, 2023).

23. Operating as designed and as implemented by Defendant, the Pixel allows the Private Information that Plaintiffs and Class Members submit to Defendant in furtherance of their health treatment to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID ("FID").¹⁰

24. Also operating as designed and implemented by Defendant, the Pixel allows the Private Information submitted by Plaintiffs and Class Members to Defendant in furtherance of their health treatment to be unlawfully disclosed to Facebook alongside a specific internet protocol ("IP") address. In these ways, among others, Defendant secretly shared personally identifying information about its Users without prior, informed consent.

25. A pixel is a piece of code that "tracks the people and [the] type of actions they take" as they interact with a website including how long a person spends on a particular web page, which buttons the person clicks, which pages they view and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box), among other things.

26. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

27. For example, when a website user visits a webpage containing Pixels, their device is commandeered, and their communications are surreptitiously duplicated and transmitted to third

¹⁰ The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser"; "[c]ookies help inform websites about the user, enabling the websites to personalize the user experience." See <https://www.cloudflare.com/learning/privacy/what-are-cookies/> (last visited May 8, 2023).

parties. Stated differently, Defendant's Website and Pixels purposely altered patients' web browsers, forcing them to duplicate and redirect HTTP requests to third-party web servers.

28. The information sent to third parties as a result of Defendant's Facebook Pixel included the Private Information that Plaintiff and Class Members submitted to Defendant's Website related to their past, present, or future health conditions, including, for example, personally identifying information, substance use disorders, symptoms, and substance use programs enrolled in.

29. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care and the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as opiate addiction or depression.

30. The third party, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who online target¹¹ Plaintiff and Class Members based on communications obtained via the Facebook Pixel and other tracking tools.

31. Simply put, by installing the Facebook Pixel on its Website, Workit effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to unknowingly disclose their confidential and extremely sensitive substance use communications to Facebook and other unauthorized third parties without their prior, informed consent.

¹¹ "Online Targeting" is "a process that refers to creating advertisement elements that specifically reach out to prospects and customers interested in offerings. A target audience has certain traits, demographics, and other characteristics, based on products or services the advertiser is promoting." See <https://digitalmarketinggroup.com/a-guide-to-online-targeting-which-works-for-your-business/> (last visited May 22, 2023).

32. In fact, an aptly named “*Out of Control*”: *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies* by The Markup and STAT recently revealed that Workit was sending patients’ “delicate, even intimate answers about drug use and self-harm to Facebook,” from the moment they started answering Defendant’s intake form.¹²

33. The Markup and STAT investigators found that the Facebook Pixel embedded on Workit’s website sent their “responses about self-harm, drug and alcohol use, and [their] Private Information—including first name, email address, and phone number—to Facebook.”¹³

34. Patients, like Plaintiffs and Class Members, simply do not anticipate that their trusted healthcare provider will send PHI or other confidential medical information to an unauthorized third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without patients’ prior, informed consent.

35. Upon information and good faith belief, in addition to the Facebook Pixel Defendant also installed and implemented Facebook’s Conversions Application Programming Interface (“CAPI”) on its Website servers.¹⁴

36. Unlike the Facebook Pixel, which coopts a website user’s browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user’s browser to transmit information directly to Facebook. Instead, CAPI tracks the user’s website

¹² See <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies> (Dec. 13, 2022) (last visited June 27, 2023).

¹³ *Id.* (noting that the trackers The Markup and STAT were able to detect and what information they sent, was “a floor, not a ceiling” and that they did not test every page on Defendant’s website).

¹⁴ “CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns.” See <https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited Jun. 20, 2023).

interaction, including Private Information, records and stores that information on the website owner's servers and then transmits the data to Facebook from the website owner's servers.^{15,16}

37. Indeed, Facebook markets CAPI as a “better measure [of] ad performance and attribution across your customer’s full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results.”¹⁷

38. Despite the clear and unequivocal prohibition on the disclosure of PHI without consent, Defendant chose to use the Pixel and CAPI data for marketing purposes in an effort to bolster its profits. That is, despite professing to “provide access to affordable, evidence-based addiction care that lowers healthcare costs and saves lives,”¹⁸ Defendant put its own desires for profit over its patients’ privacy rights.

39. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build robust profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs’ and Class Members’ Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

¹⁵ See <https://revealbot.com/blog/facebook-conversions-api/> (last visited Jun. 20, 2023).

¹⁶ “Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel... This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.” <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited Jun. 20, 2023).

¹⁷ Because CAPI is located on the website owner’s servers and is not a bug planted onto the website user’s browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users’ Private Information to Facebook directly. See <https://www.facebook.com/business/help/2041148702652965?id=818859032317965> (last visited Jun. 20, 2023).

¹⁸ <https://www.workithealth.com/> (last visited Jun. 27, 2023).

40. The information that Defendant’s Pixel and CAPI sent to Facebook included the Private Information that Plaintiffs and Class Members submitted to Defendant’s Website, including for example, the type of medical treatment sought, the individual’s particular substance addiction, details of their drug or alcohol use, and the fact that the individual attempted to or did book a medical appointment.

41. It is not difficult to imagine what use a social media company might have for tracking a person who is struggling with their mental health (especially in connection with substance abuse), and how often they seek therapy: in 2017, a leaked Facebook sales pitch showed the company boasting of how its algorithm could identify and target teenagers who were feeling “insecure” and “worthless,” “overwhelmed” or “anxious.”

42. Moreover, there is unfortunately a lot of stigma in struggling with drug and alcohol abuse. Such data sharing could be particularly damaging to patients seeking care for substance use disorders, among many other problematic outcomes for users.¹⁹

43. In fact, experts worry that health data could be used to target patients in need with ads for services and therapies that are unnecessary or even harmful.²⁰

44. Neither Plaintiffs nor any other Class Member signed a valid written authorization permitting Workit to send, sell, or otherwise profit from their Private Information to Facebook or Google.

¹⁹ See Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), available at <https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last visited June 27, 2023) (“While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it’s even more verboten in addiction treatment, as patients’ medical history can be inherently criminal and stigmatized.”).

²⁰ “*Out of Control*,” note 12, *supra*.

45. Despite willfully and intentionally incorporating the Facebook Pixel and Google Analytics into its Website, Workit has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook, Google, or other third-party advertisers.

46. Defendant's unilateral disclosure of such private information is unquestionably a violation of HIPAA, among other statutory and common laws.

47. Workit owed common law, statutory, and regulatory duties to keep Plaintiffs' and Class Members' Private Information safe, secure and confidential.

48. Furthermore, by obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

49. As detailed herein, Workit breached its statutory, common law, and equitable obligations to Plaintiffs and Class Member by, *inter alia*: (i) failing to review its marketing programs and web based technology to ensure the safety and security of its Website; (ii) failing to remove or to disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the prior, informed, and written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook, Google, and/or others; (iv) failing to take steps to block or restrict the transmission of Plaintiffs' and Class Members' Private Information through Facebook Pixels and/or other tracking tools; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of its Users' Private Information.

50. As a result, Plaintiffs and Class Members have suffered numerous injuries and damages, including but not limited to: (i) invasion of privacy; (ii) loss of confidentiality; (iii) being

subjected to unsolicited and unwanted advertisements targeting them because of Defendant's unlawful conduct; (iv) loss of benefit of the bargain; (v) diminution of value of the Private Information; (vi) emotional distress; (vii) loss of property interest in their personal data; (viii) nominal damages; (ix) punitive damages; and/or (x) statutory damages.

PARTIES

51. Plaintiff Jane Doe 1 is an individual natural person that is over the age of 18 years old who is, and at all relevant times was, a resident and a citizen of Hocking County, State of Ohio. Plaintiff received healthcare services from Defendant beginning approximately April 2021 and accessed those services via Defendant's Website. While using Defendant's Website, Plaintiff communicated sensitive, and what she presumed to be confidential, personal and medical information to Defendant. Plaintiff seeks to proceed under a pseudonym in this Action due to the private nature of her Private Information and privacy-related claims.

52. Plaintiff Jane Doe 2 is an individual natural person that is over the age of 18 years old who is, and at all relevant times was, a resident and a citizen of Riverside County, State of California. Plaintiff received healthcare services from Defendant beginning approximately October 2021 and accessed those services via Defendant's Website. While using Defendant's Website, Plaintiff communicated sensitive, and what she presumed to be confidential, personal and medical information to Defendant. Plaintiff seeks to proceed under a pseudonym in this Action due to the private nature of her Private Information and privacy-related claims.

53. Defendant Workit Health Inc. is a Delaware Corporation with its principal place of business in Michigan, at 3300 Washtenaw Avenue, Suite 280 Ann Arbor, Michigan 48104. Defendant maintains a registered office at 3410 Belle Chase Way, Suite 600, Lansing, Michigan 48911. Defendant developed, owns, and/or operates its Website.

54. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d, 45 C.F.R. Part 160-45 C.F.R. Part 162, & 45 C.F.R. Part 164 (“HIPAA”).

JURISDICTION & VENUE

55. This Court has subject matter jurisdiction over this action further to 28 U.S.C. § 1331 because it arises under the laws of the United States.

56. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because the operative Complaint alleges questions of federal law under the ECPA (28 U.S.C. § 2511, et seq.).

57. This Court has original jurisdiction under 28 U.S.C. § 1332(a)(1) because the amount in controversy greatly exceeds \$75,000, exclusive of interests and costs, and there is a complete diversity of citizenship between the parties.

58. Separately, and in addition to diversity jurisdiction under 28 U.S.C. § 1332(a)(1), this Court has original subject matter jurisdiction pursuant to the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d). CAFA jurisdiction is appropriate because at least one member of the proposed class is a citizen of a different State from Defendant, there are 100 or more Class Members, and the aggregate amount in controversy exceeds five million dollars (\$5,000,000.00), exclusive of interest and costs.

59. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 because the state law claims alleged herein are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

60. This Court has personal jurisdiction over Defendant because its principal place of business is in this judicial district and a substantial portion of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this judicial district.

61. Venue is proper in this Court because Defendant is a resident of Michigan, with its principal place of business in the Eastern District of Michigan.

COMMON FACTUAL ALLEGATIONS

Background: The Use of Tracking Technologies in the Healthcare Industry

62. Tracking tools²¹ installed on many hospitals, telehealth companies' and other healthcare providers' websites (and other digital properties) are collecting patients' confidential and private health information—including details about their medical conditions, prescriptions and appointments, among many other things—and sending that information to third party platforms without prior, informed consent.²²

63. These pixels are snippets of code that track users as they navigate through a website, logging which pages they visit, which buttons they click and certain information they enter into forms. In exchange for installing the pixels, the third-party platforms (e.g., Facebook and Google)

²¹ The OCR has defined such “tracking technology” as a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app. After information is collected through tracking technologies from websites or mobile apps, it is then analyzed by owners of the website or mobile app (“website owner” or “mobile app owner”), or third parties, to create insights about users' online activities. *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>, HHS.GOV (last visited June 4, 2023).

²² *See, e.g.*, Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), available at <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited May 22, 2023).

provide website owners analytics about the advertisements they have placed as well as tools to target people who have visited their web properties.

64. While the information captured and disclosed without permission by a medical entity's website may vary depending on the pixel(s) embedded, these "data packets" can be extensive, sending, for example, not just the user's medical condition, treatment sought, patient status, the services or programs enrolled in, type and date of their medical appointments, the name of the physician and her field of medicine, exact words and terms typed into a search bar, text of buttons clicked, but also the first name, the last name, email address, phone number and zip code, city of residence, and any other Private Information the user enters into the booking form.

65. That data is linked to a specific internet protocol ("IP") address which can be tracked to a particular household and, together with other technical data, to a particular person.

66. The Facebook Pixel, for example, sends information to Facebook via scripts running in a person's internet browser so each data packet comes labeled with an IP address that can be used in combination with other data to identify an individual or household.

67. In addition, if the person is (or recently has) logged into Facebook when they visit a particular website when a Facebook Pixel is installed, the browsers will attach cookies—another tracking mechanism—that allow Facebook to link pixel data to specific, unique Facebook accounts.²³

²³ Investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' Private Information. Specifically, and for example, The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment; and 49 out of 50 telehealth startups investigated (including Workit) sent URLs users visited on the startup's site and their IP address to at least one Big Tech company. See <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>; <https://themarkup.org/pixel-hunt/2022/12/13/out->

Facebook's Business Tools & The Pixel

68. Facebook operates the world's largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.²⁴

69. Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target and market products and services to individuals.

70. Facebook's Business Tools, including the Pixel and CAPI, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers thereby enabling the interception and collection of Users' data on those platforms.

71. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.

72. Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."

73. One such Business Tool is the Pixel which "tracks [] people and [the] type of actions they take."²⁵ When a user accesses a webpage that is hosting the Pixel, their communications with the host webpage are instantaneously (and surreptitiously) duplicated and sent to Facebook's servers—traveling from the User's browser to Facebook's server.

[of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.](#)

²⁴ FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited May 22, 2023).

²⁵ FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited May 22, 2023).

74. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via the Pixel but for Defendant's decisions to install the Pixel on its Website.

75. Similarly, Plaintiffs' and Class Member's Private Information would not have been disclosed to Facebook via CAPI but for Defendant's decision to install and to use that tool.

76. By installing and implementing both tools, Defendant caused Users' communications (including, but not limited to, Private Information) to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via CAPI.

77. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via the Website.

Defendant's Method of Transmitting Plaintiffs' & Class Members' Private Information via the Tracking Pixel and/or CAPI

78. Web browsers are software applications that allow consumers to navigate the web and to view and to exchange electronic information and communications over the internet.

79. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser and Microsoft's Edge browser).

80. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet Users' client devices via their web browsers.

81. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request:** an electronic communication sent from the client device’s browser to the website’s server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies:** a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are “third-party cookies” which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response:** an electronic communication that is sent as a reply to the client device’s web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.²⁶

82. A User’s HTTP Request essentially asks the Defendant’s Website to retrieve certain information (such as a physician’s “Book an Appointment” page), and the HTTP Response renders or loads the requested information in the form of “Markup” (the pages, images, words, buttons and other features that appear on the User’s screen as they navigate Defendant’s Website).

83. Every website is comprised of Markup and “Source Code.” Source Code is simply a set of instructions that commands the website visitor’s browser to take certain actions when the web page first loads or when a specified event triggers the code.

84. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser’s user. Defendant’s Pixel and Google Analytics tracking technology is source code that does just that. The Pixel and Google Analytics acts much like a traditional wiretap.

²⁶ One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

85. When patients visit Defendant's website via an HTTP Request to Workit's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including the Pixel and Google Analytics tracking technology.

86. Thus, Defendant is in essence handing patients a tapped phone and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage (or other digital property) to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to unauthorized third parties, including Facebook and Google.

87. Third parties, like Facebook, place third-party cookies in the web browsers of users logged into their platforms. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can identify the patient associated with the Private Information intercepted.

88. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology; that is why third parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users.

89. Facebook's workaround, for example, is called Conversions API, which is an effective workaround because it does not intercept data communicated from the user's browser. Instead, CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."

90. Thus, the private communications between Users and ProHealth, which are necessary to use its Web Properties, are actually received by Defendant and stored on its server before CAPI collects and sends the Private Information contained in those communications directly from Defendant to Facebook.

91. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

92. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to “[u]se the CAPI in addition to the [] Pixel, and share the same events using both tools” because such a “redundant event setup” allows Defendant “to share website events [with Facebook] that the pixel may lose.”²⁷

93. Thus, without any knowledge, authorization, or action by a User, a website owner like Defendant can use its source code to commandeer the user’s computing device, causing the device to contemporaneously and surreptitiously re-direct Users’ communications to third parties.

94. In this case, Defendant employed the Facebook Pixel and CAPI (and other tracking codes) to intercept, duplicate and re-direct Users’ Private Information to Facebook and other third parties along with personally identifying information.

95. For example, when a patient visits <https://www.workithealth.com/> and clicks “Get Addiction Treatment” and “Meth Addiction”, the patient’s browser automatically sends an HTTP Request to Defendant’s web server. The Defendant’s web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted below:

²⁷ See <https://www.facebook.com/business/help/308855623839366?id=818859032317965> (last visited Jun. 20, 2023).

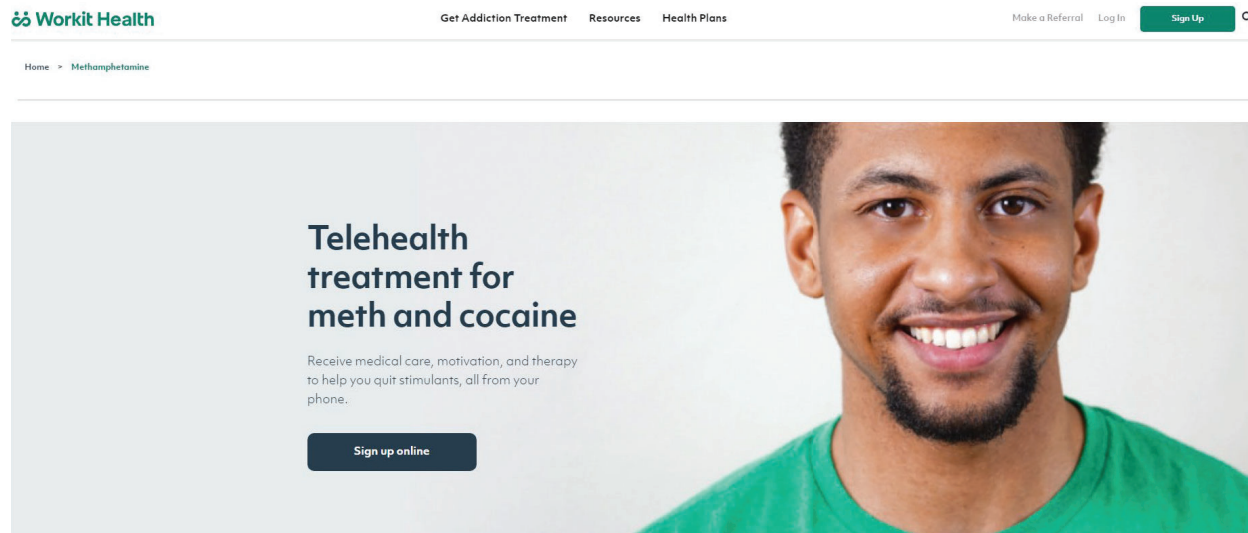


Figure 1. Image taken from <https://www.workithealth.com/methamphetamine/>

96. The patient visiting this web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses.

97. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via pixels or web bugs,²⁸ effectively opening a spying window through which the webpage can funnel the visitor's data, actions and communications to third parties.

98. Looking to the previous example, Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and to send those communications to Facebook, including full string URLs containing the webpages visited by the User, terms entered into search fields and fillable forms, button click data and keystrokes.

²⁸ These pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

99. This occurs because the Pixel and Google tracking technology embedded in Workit's Source Code is programmed to automatically track and to transmit Users' communications, and this occurs contemporaneously, invisibly and without patient knowledge.

100. Thus, without consent, Defendant has effectively used its source code to commandeer patients' computing devices thereby re-directing their Private Information to third parties.

101. The information that Defendant's Pixel sends to Facebook includes, among other things, patients' PII, PHI, and other confidential information.

102. Upon information and good faith belief, Defendant's Pixel sent non-public Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) sought treatment or therapies; (4) appointment requests and appointment booking information; (5) registration or enrollment in programs (such as opioid use disorder programs) (6) Private Information including first name, email, phone number, and zipcode; (7) details of their drug and/or alcohol use; (8) medications; (9) phrases and search queries conducted via the general search bar and (10) which webpages were viewed.

103. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiffs' and Class Members' Facebook ID (c_user cookie or FID), thereby allowing individual Users' communications with Defendant, and the Private Information contained in those communications to be linked to their unique Facebook accounts.

104. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily

use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie or FID, one simply needs to type www.facebook.com/ followed by the c_user ID.

105. Also, the Private Information Defendant's Pixel sent to Facebook is sent alongside an IP Address, thereby allowing individual patients' communications with Defendant, and the private information contained in those communications to be linked to their unique devices.

106. Defendant deployed other invisible tracking tools on its Website, which also collected dozens of data points about individual website users who utilized its services and caused users' Private Information to be shared with Google, Bing, and Twitter.

Defendant's Website Disseminates Users Private Information via www.workithealth.com/

107. Defendant is a telehealth provider of substance use disorder treatment services, in addition to certain mental health services.

108. Thousands of individuals visit Defendant's Website each year, in order to receive information, diagnoses, and/or treatment regarding addiction or mental health conditions.

109. Individuals use Defendant's Website to search for medical information, diagnosis, treatment, programs, appointments, and/or services relating to addiction and/or mental health conditions.

110. Workit claims to help its patients "Quit opioids or alcohol from the privacy of home" and to provide "personalized treatment and seamless care right to your fingertips with the convenience of an app."²⁹

²⁹ See <https://www.workithealth.com/> (last visited June 27, 2023).

111. Workit combines online individual and group therapy along with medication-assisted treatment. In addition, the company claims that their “world-class care provides integrated treatment and support for co-occurring disorders.”³⁰

112. In the process, Workit collects a treasure trove of personal data.

113. On Workit’s Website, patients get started by answering questions about their substance use and mental health, ostensibly to help Workit determine which program is right for them. What Workit is secretly doing is mining Users’ data and using it for its own impermissible business purposes.

114. Before Users provide any Private Information to Defendant, Defendant affirmatively and prominently promises Users that “All of the information you share is kept private and is protected by our HIPAA-compliant software.”³¹

Sign up for Workit Health

Get started by answering a few questions to help us determine which program is right for you. All of the information you share is kept private and is protected by our HIPAA-compliant software.

Continue

115. However, this claim could not be further from the truth.

³⁰ See <https://www.workithealth.com/co-occurring-disorders/> (last visited June 27, 2023).

³¹ <https://app.workithealth.com/signup> (last visited June 27, 2023).

116. After Workit users, including Plaintiffs, clicked on the “Continue” button to sign up with Defendant, the “Start your Workit profile” page once again assured Users that “We take your privacy seriously. Your information is protected by our HIPAA compliant software.” Defendant’s statement prominently encouraged users to provide personal and admittedly HIPAA-protected information to Defendant prior to signing up, with assurances that any private information they provide will be kept private.³²

Start your Workit profile

First Name (Preferred) (Required)

Date of Birth (Required)

ZIP/Postal Code (Required)

How did you hear about us? (Required)

Continue

We take privacy seriously. Your information is protected by our HIPAA compliant software. [Learn more about our privacy practices.](#)

Already scheduled an appointment over the phone? [Activate account](#)

Already have an account? [Sign in](#)

117. Defendant then requires Users to enter personal information into its Website, including how the User heard about Workit, and the type of services sought and before they can

³² https://app.workithealth.com/onboarding/zip_code (last visited June 27, 2023).

register for an account with a unique login and password. This information includes Name, Date of Birth, Zip/Postal Code, and how each User heard about Workit.³³

118. This information – including patients’ answers to medical questionnaires, name, email address, phone number, as well as information about medical products they purchase on Workit’s website – was sent to advertising platforms, along with the information needed to identify users.³⁴

119. Such data is highly personal and can be used to target advertisements for services that may be unnecessary or that may be “potentially harmful physically, psychologically, or emotionally.”³⁵

120. Only after all of this personal information is provided does Workit require Users to agree to Defendant’s Terms of Service and Privacy Policy. Workit privacy policies represent that it has put in place appropriate physical, electronic, and administrative safeguards in compliance with federal and state law, including HIPAA, and promise its users that Workit will “not disclose Personal Information that we collect on the Service to third parties without your consent.” In

³³ Defendant expressly asks each User to provide details about how they found out about Workit Health. For example, if a User clicks “Social Media/Advertisement,” Workit specifically asks whether the ad was viewed on “Facebook, “Google” or “Other.” This demonstrates that Defendant is using its intake form to monitor the performance of its advertisements on Facebook and Google, the very sites where it discloses Users’ Private Information for marketing purposes. This also supports Plaintiffs’ allegation that Defendant’s collection and dissemination of data is pursuant to its own profit motives and unrelated to any permissible medical purpose for violating Plaintiffs’ privacy without prior, informed consent. See https://app.workithealth.com/onboarding/zip_code (last visited June 27, 2022).

³⁴ See <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>.

³⁵ See *id.*; see also <https://www.commerce.senate.gov/2023/2/cantwell-klobuchar-collins-lummis-call-on-telehealth-companies-to-protect-patients-sensitive-health-data> (last visited June 27, 2023).

instances where it uses Personal Information collected through patient's use of the Service for enumerated reasons, including advertising, any such disclosures allegedly take place only after a patient consents to them doing so.³⁶

121. However, unbeknownst to Plaintiffs and Class Members, Defendant had embedded an undetectable tracking Pixel and CAPI tracking tools into its Website, which automatically transmitted to Facebook every click, keystroke and intimate detail about their Private Information, medical symptoms, conditions and treatments, and disclosed it to Facebook along with personal identifying information, including Users' FID and/or other personally identifying information.

122. Defendant's Website collects various information about its users including, but not limited to:

- a) The type of medical treatment a User is seeking;
- b) A User's Health conditions;
- c) A User's registration or enrollment in specific programs;
- d) Location of facilities where User signed up for or sought treatment;
- e) The appointment type and date;
- f) A User's specific menu selections;
- g) Content typed into free boxes (such as searches for symptoms, programs, or treatment options);
- h) Demographic information;
- i) Contact information (email addresses, phone numbers, etc.);
- j) Emergency contact information;
- k) The webpages the User viewed;
- l) Any phrases and search queries a User entered via general search bar.

123. The information provided by users to Defendant constitutes Private Information.

124. For example, information entered into Defendant's Website indicating their recent alcohol use is simultaneously, and without prior, informed consent of the User, sent to Facebook—

³⁶ See <https://app.workithealth.com/signup> (last visited June 27, 2023); see also Workit privacy policies, available at <https://www.workithealth.com/privacy-policy/> and <https://www.workithealth.com/hipaa-notice/> (last visited June 27, 2023).

along with the User’s Facebook ID and personal information including first name, zipcode, email, and phone number:

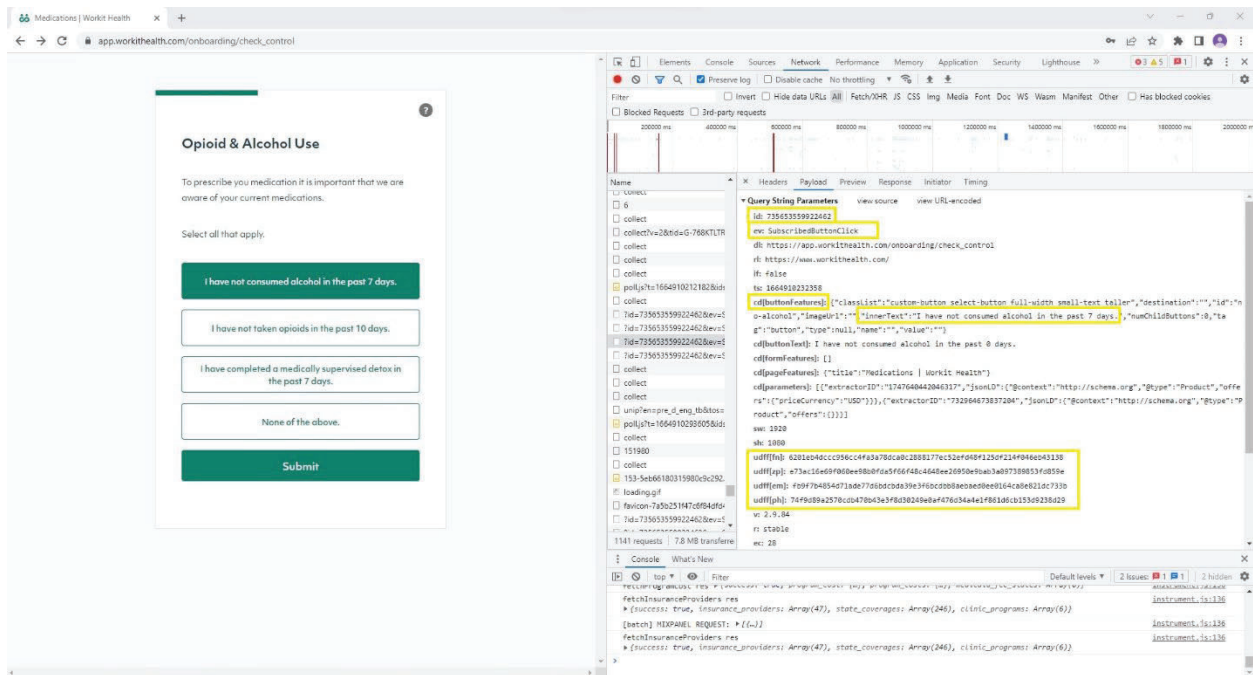


Image taken from The Markup and STAT’s database of images collected during their investigation of 50 telehealth companies’ data tracking practices, available at <https://github.com/the-markup/investigation-d2c-privacy>³⁷

125. The first line (highlighted in yellow) under “Query String Parameters”, “id: 735653559922462,” refers to Defendant’s Pixel ID for this particular Webpage and confirms that Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

³⁷ According to The Markup and STAT, after the investigators contacted Workit to share their findings of data collection and disclosure, Workit changed its use of trackers. When The Markup and STAT tested the Website again on December 7, 2022, they did not find evidence of tech platform tracking tools during Defendant’s intake or checkout process. See <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>. Due to Workit having removed the Pixel prior to the publication of the results of the investigation which made these illegal practices public knowledge, Plaintiffs could not capture Defendant’s tracking tools and rely on information gathered during The Markup and STAT’ investigation.

126. The second line of text in this section, “ev: SubscribedButtonClick” identifies and categorizes which actions the User took on the Webpage (“ev:” is an abbreviation for event, and “SubscribedButtonClick” is the type of event). Thus, this identifies the User as having clicked on a particular button on Defendant’s Webpage.

127. The seventh and eight lines show the inner text of the button the User clicked, here, “I have not consumed alcohol in the past 7 days.”

128. Lines eighteen through twenty-one show hashed personal information that was collected by Defendant via its intake form (the User’s first name, zip code, email, and phone number) and is being disclosed to Facebook.

129. While hashing obscures those details into a string of letters and numbers, it does not prevent tech platforms from linking them to a specific person’s profile for advertising purposes, which Facebook explicitly says it does before discarding the hashed data.

130. Workit was sharing all information collected by its intake form during the User’s intake process, For example, Defendant shared with Facebook the User’s insurance information, along with other personal information and unique personal identifiers:

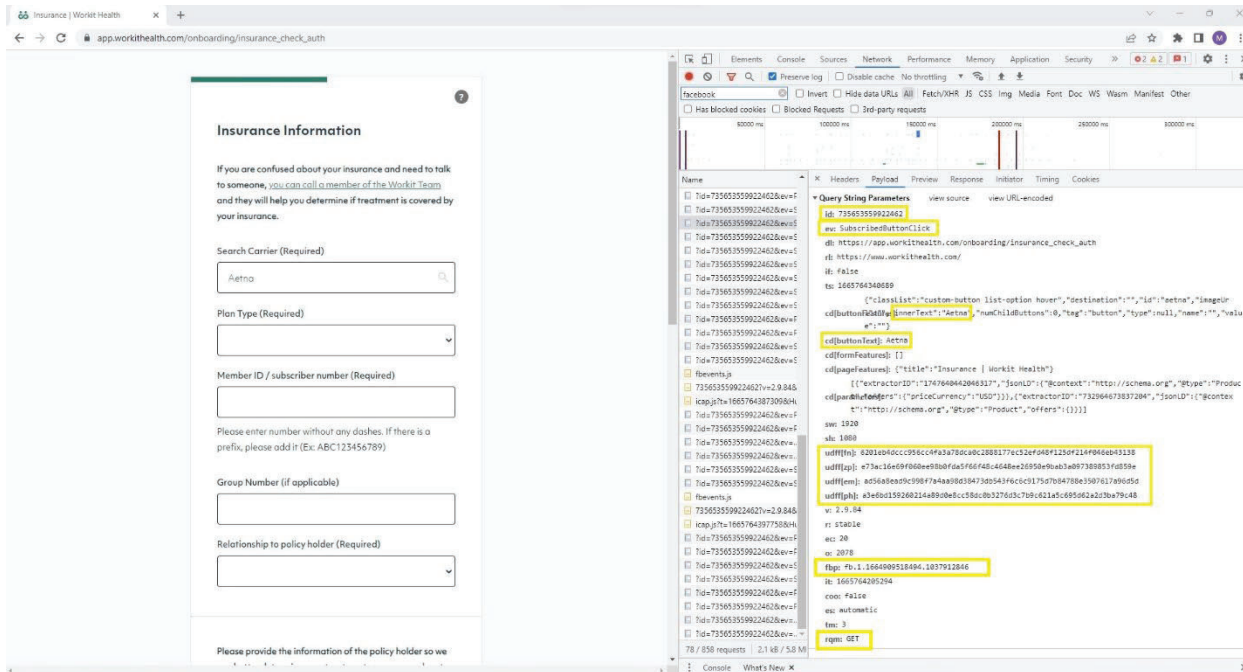


Image taken from The Markup and STAT’s database of images collected during their investigation of 50 telehealth companies’ data tracking practices, available at <https://github.com/the-markup/investigation-d2c-privacy>

131. Lines eight and ten of the text identify the User’s insurance information, which the User submitted to Defendant as part of the insurance check. Line three shares the URL where the User took the identified action (https://app.workithealth.com/onboarding/insurance_check_auth).

132. Again, Defendant is sharing the User’s first name, zip code, email and phone number.

133. Line twenty-six shows that Defendant also utilizes the `_fbp` cookie, which Facebook uses to identify a browser and a user, as discussed *infra*.

134. Finally, the last line of the text (`rqm: GET`), demonstrates that Defendant’s Pixel sent the User’s communications (and the Private Information contained therein) alongside the User’s Facebook ID (`c_userID`).

135. While the data captured by the Markup and STAT does not show the c_user cookie in this instance (it would be disclosed in the “Headers” part of the data inspection tool used, not in the “Payload”), upon information and good faith belief, a user who accessed Defendant’s website while logged into Facebook did transmit the c_user cookie to Facebook, which contains that User’s unencrypted Facebook ID.

136. This is supported by data from Plaintiffs’ “Off-Facebook Activity” logs which show activity from the businesses and organizations one visits off of Facebook, and which show interactions between Facebook and Workit.

137. Each time Workit sent this activity data, it also disclosed a patient’s personally identifiable information alongside the contents of their (supposedly private) communications.

138. Cookies are considered PII, and tracking pixels can collect cookies from website visitors.

139. “Session cookies” are placed on a user’s computing device only while the user is navigating the website that placed and accesses the cookie. The user’s web browser typically deletes session cookies when the user closes the browser.

140. “Persistent cookies” are designed to survive beyond a single internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can acquire and record a user’s internet communications for years and over dozens or even hundreds of websites. Persistent cookies are also called “tracking cookies.”

141. Cookies are also classified by the party that uses the collected data.

142. “First-party cookies” are set on a user’s device by the website with which the user is exchanging communications. First-party cookies can be helpful to the user, server, and/or website to assist with security, login, and functionality.

143. “Third-party cookies” are set on a user’s device by website servers other than the website or server with which the user is exchanging communications. For example, the same patient who visits Defendant’s website will also have cookies on their device from third parties, such as Facebook and Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies are typically used for data collection, behavioral profiling, and targeted advertising.

144. Data companies like Facebook have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell advertising that is customized to a user’s communications and habits. To build individual profiles of internet users, third party data companies assign each user a unique identifier or set of unique identifiers.

145. Traditionally, first party and third-party cookies were kept separate. An internet security policy known as the same-origin policy required web browsers to prevent one web server from accessing the cookies of a separate web server. For example, although Defendant can deploy source code that uses Facebook third-party cookies to help Facebook acquire and record a patient’s communications, Defendant is not permitted direct access to Facebook third-party cookie values. The reverse was also true: Facebook was not provided direct access to the values associated with first-party cookies set by companies like Defendant. But data companies have designed a way to hack around the same-origin policy so that third-party data companies like Facebook can gain access to first-party cookies.

146. JavaScript source code developed by third party data companies and placed on a webpage by a developer such as Defendant can bypass the same-origin policy to send a first-party cookie value in a tracking pixel to the third-party data company. This technique is known as

“cookie synching,” and it allows two cooperating websites to learn each other’s cookie identification numbers for the same user. Once the cookie synching operation is completed, the two websites can exchange any information that they have collected and recorded about a user that is associated with a cookie identifier number. The technique can also be used to track an individual who has chosen to deploy third-party cookie blockers.

147. In effect, cookie synching is a method through which Facebook, Google, and other third-party marketing companies set and access third-party cookies that masquerade as first-party cookies. By designing these special third-party cookies that are set for first-party websites, Facebook and Google hack their way around any cookie blockers that users set up to stop their tracking.

148. Upon information and good faith belief, when accessing Defendant’s Website, Facebook received several cookies, including but not limited to the `c_user` and the `_fbp` cookies.

149. The `_fbp` cookie, which Facebook uses to identify a browser and a user, attaches to a browser as a first-party cookie.³⁸

150. The `_fbp` cookie expires after 90 days unless the visitor’s browser accesses the same website.³⁹ If that happens, the time resets, and another 90 days begins to accrue.

151. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is “created by the website the user is visiting”—i.e., Defendant.⁴⁰

³⁸ *Cookies & other storage technologies*, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited Jun. 20, 2023).

³⁹ *Cookies & other storage technologies*, FACEBOOK.COM, <https://www.facebook.com/policy/cookies/> (last visited Jun. 20, 2023).

⁴⁰ *First-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited Jun. 20, 2023). This is confirmable by using developer tools to inspect a website’s cookies and track network activity.

152. A third-party cookie is “created by a website with a domain name other than the one the user is currently visiting”—i.e., Facebook.⁴¹

153. The `_fbp` cookie is always transmitted as a first-party cookie. A duplicate `_fbp` cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

154. The `_fbp` cookie is also a third-party cookie in that it is also a cookie associated with Facebook that is used by Facebook to associate information about a person and their communications with non-Facebook entities while the person is on a non-Facebook website or app.

155. If a User takes an action to delete or clear third-party cookies from their device, the `_fbp` cookie is not impacted—even though it is a Facebook cookie—because Facebook has disguised it as a first-party cookie. Facebook also uses IP addresses and user-agent information to match the health information it receives from Defendant with Facebook users.

156. Defendant engages in cookie synching with Facebook, Google, and other third parties.

157. Defendant uses and causes the disclosure of patient cookie identifiers with each re-directed communication described herein, including patient communications concerning individual providers, conditions, and treatments.

158. Facebook, at a minimum, uses the `_fbp` and `c_user` cookies to link to FIDs and corresponding Facebook profiles.

⁴¹*Third-Party Cookie*, PCMAG.COM, <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited Jun. 20, 2023). This is also confirmable by tracking network activity.

159. As shown in the above images, and upon information and good faith belief, Defendant sent these identifiers with the event data.

160. Another category of personally identifiable information protected by law against disclosure are unique user identifiers (such as Facebook’s “Facebook ID”) that permit companies like Facebook to quickly and automatically identify the user’s personal identity across the internet whenever the identifier is encountered. A Facebook ID is an identifying number string that is connected to a user’s Facebook profile.⁴² Anyone with access to a user’s Facebook ID can locate a user’s Facebook profile.⁴³

161. As discussed above, the Pixel embedded on Defendant’s Website collected and shared with Facebook these unique identifiers as well.

162. Although the full scope of Defendant’s illegal data sharing practices is presently unknown, additional evidence demonstrates that Defendant was also sharing its Users’ IP addresses alongside a patient’s communications and data, with Facebook and other big tech companies.⁴⁴

163. An IP address is a number that identifies the address of a device connected to the Internet.

164. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

165. Facebook tracks every IP address ever associated with a Facebook user.

⁴² <https://www.facebook.com/help/211813265517027> (last visited June 21, 2023).

⁴³ <https://smallseotools.com/find-facebook-id/> (last visited June 21, 2023).

⁴⁴ See <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>.

166. Google also tracks IP addresses associated with Internet users.

167. Facebook, Google, and other third-party marketing companies track IP addresses for use of tracking and targeting individual homes and their occupants with advertising by using IP addresses.

168. Under HIPAA, an IP address is considered PHI. See 45 C.F.R. § 164.514 (2).

169. HIPAA further declares information as personally identifiable where the covered entity has “actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.” 45 C.F.R. § 164.514(2)(ii); See also, 45 C.F.R. § 164.514(b)(2)(i)(O).

170. Consequently, Defendant’s disclosure of patients’ IP addresses violated HIPAA and industry privacy standards.

171. On February 2, 2023, four members of the United States Senate sent a letter to Workit where they expressed “concern regarding reports that Workit is tracking and sharing sensitive and personally identifiable health data with third-party social media and online search platforms such as Google and Facebook that monetize this data to target advertisements.”⁴⁵

172. Workit has not only ignored these concerns, but it has repeatedly broken its aforementioned privacy promises—as well as federal and state privacy laws—by using its users’ and patients’ data for various purposes including advertising, its own and by third parties.

⁴⁵ See <https://www.commerce.senate.gov/2023/2/cantwell-klobuchar-collins-lummis-call-on-telehealth-companies-to-protect-patients-sensitive-health-data> (last visited June 27, 2023).

173. As was just admitted by another online mental health platform, Cerebral, such practices constitute unlawful disclosures of patient health data.⁴⁶

174. Thousands⁴⁷ of consumers like Plaintiffs have entrusted Workit with their addiction status, information about their mental health and medical history, and various personal identifiers including the user's name, email and IP addresses, and phone number.

175. It cannot be disputed that visitors and users of addiction treatment services want to keep their information private.

176. Workit realized and acknowledged that this information is sensitive and it should be protected from disclosure unless the user gives their express written consent.

177. However, Workit's assurances that it will keep Users' medical information confidential were deceptive and false.⁴⁸

178. Workit violated HIPAA, the HIPAA Privacy Rule, the HHS Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates bulletin, and

⁴⁶ Bleeping Computer, "Mental health provider Cerebral alerts 3.1M people of data breach," March 10, 2023, available at <https://www.bleepingcomputer.com/news/security/mental-health-provider-cerebral-alerts-31m-people-of-data-breach/> (last visited June 27, 2023).

⁴⁷ [Lindsay Kalter](#), *Ann Arbor Startup Workit Health Is on Its Way to Unicorn Status*, HOUR DETROIT (April 12, 2022), available at <https://www.hourdetroit.com/health/ann-arbor-startup-workit-health-is-on-its-way-to-unicorn-status/> (last visited June 27, 2023).

⁴⁸ In addition to making false representations, Workit has pushed visitors and users into handing over their health information before they have ever had a chance to read any privacy disclosures. Upon visiting any of Workit webpages, visitors are urged to begin the Intake Questionnaire and hand over their health information. By contrast, Workit links to the privacy policy do not appear on any of the intake pages and can only be found at the very bottom of the website on the pages that urge visitors to sign up.

Workit's own Privacy Policy and Notice of Privacy Practices, by sharing users' health information with third-party advertising platforms such as Facebook and Google.⁴⁹

179. Workit broke its privacy promises to monetize consumers' Private Information and to target them and others with advertisements for its Service, by installing third-party tracking codes on its digital properties (including but not limited to, the Meta Pixel and Google Analytics). In handing over its users' sensitive medical data to third-party advertising platforms, Workit permitted those companies to use this information for their own research and product development, without limitation and without Users' prior, informed consent.

180. In addition, Workit failed to employ reasonable measures to safeguard the health information it collected from consumers. Workit did not properly train its employees on how to protect the information when using it for advertising, and Workit did not properly supervise its staff in the use of the information.

181. Workit also failed to provide consumers with proper notice as to the collection, use, and disclosure of their health information.

182. Defendant has also failed to take reasonable steps to anonymize the Private Information it disseminated to Facebook and Google through the Pixel and Google Analytics.

183. Last, but not least, Workit failed to limit contractually how third parties could use consumers' health information, instead merely agreeing to their stock contracts and terms.

⁴⁹ For example, Workit privacy policies represent that it has put in place appropriate physical, electronic, and administrative safeguards in compliance with federal and state law, including HIPAA, and promise its users that Workit will "not disclose Personal Information that we collect on the Service to third parties without your consent." In instances where it uses personal information collected through patient's use of the Service for enumerated reasons, including advertising, any such disclosures allegedly take place only *after* a patient consents to them doing so. See Workit privacy notices, *supra* note 26.

184. Defendant's use of the Facebook Pixel and Google Analytics to disclose Users' Private Information is a common policy and practice that Defendant utilized to secretly, and without prior, informed consent, monetize Plaintiffs' Private Information for its own gain.

Tracking Technologies on Healthcare Websites Violate the HIPAA Privacy Rule

185. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates 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 either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

186. HIPAA prohibits health care providers from "us[ing] or disclos[ing] 'protected health information "except as permitted or required by" the HIPAA Privacy Rule. 45 C.F.R. § 164.502.

187. "A covered entity may determine that health information is not individually identifiable health information only if" either "a person with appropriate knowledge of and experience with generally accepted statistical and scientific methods for rendering information not individually identifiable: a) applying such principles" determines that the risk is "very small" that the information could be used alone, or in combination with other information, to identify individuals, and documents the methods that justifies such a determination, or identifiers are removed that include: Internet Protocol (IP) address numbers; account numbers; URLs, device identifiers, and "any other unique identifying number, characteristic or code," except codes assigned by the healthcare organization to allow itself to reidentify information from which it has

removed identifying information. See 45 C.F.R. § 160.514.

188. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. See 45 C.F.R. §§ 160.103, 164.502.

189. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

190. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

191. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

192. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be Protected Health Information.

193. The Department of Health and Human Services has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data:

If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.⁵⁰

194. Consistent with this restriction, HHS has issued marketing guidance that provides that: “With limited exceptions, the [Privacy] Rule requires an individual’s written authorization before a use or disclosure of his or her protected health information can be made for marketing. . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party’s own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.”⁵¹

195. Defendant’s placing of third-party tracking code on its Website is a violation of Plaintiffs’ Class Members’ privacy rights under federal law. While Plaintiffs do not bring a claim under HIPAA itself, this violation evidences Defendant’s wrongdoing as relevant to other claims.

Federal Warning on Tracking Codes on Healthcare Websites

196. The government has issued guidance reminding healthcare entities that tracking code like the Facebook Pixel may violate federal privacy law when installed on healthcare websites.

197. That guidance, titled *Use of Online Tracking Technologies By HIPAA Covered*

⁵⁰[HHS.gov, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT \(HIPAA\) PRIVACY RULE,](https://www.hhs.gov/hipaa/forprofessionals/privacy/special-topics/de-identification/index.html) <https://www.hhs.gov/hipaa/forprofessionals/privacy/special-topics/de-identification/index.html> (last visited Jun. 20, 2023).

⁵¹[HHS.gov, MARKETING,](https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/marketing/index.html) <https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/marketing/index.html> (last visited Jun. 20, 2023).

Entities And Business Associates (the “Bulletin”), was recently issued by the HHS OCR.⁵²

198. Healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Facebook Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients’ protected health information to these vendors. The Bulletin explains:

Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. *For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.*⁵³

199. The bulletin discusses the types of harm disclosure may cause:

An impermissible disclosure of an individual’s PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. *For example, an impermissible disclosure of PHI 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 identified in the individual’s PHI.* Such disclosures can reveal incredibly sensitive information about an individual, *including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.* While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, *because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*⁵⁴

⁵² [HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html) (last visited Jun. 20, 2023).

⁵³ *Id.* (emphasis added).

⁵⁴ *Id.* (emphasis added).

200. Plaintiffs and Class members face just the risks about which the government expresses concern.

201. As detailed herein, Defendant has disclosed Plaintiffs' and Class Members' medical conditions, patient status as someone seeking substance abuse treatment, details of their drug and/or alcohol use, and various unique personal identifiers.

202. This information is, as described by the OCR in its bulletin, "highly sensitive."

203. The Bulletin goes on to make clear how broad the government's view of PHI is:

This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code.⁵⁵

204. Crucially, that paragraph in the government's Bulletin continues:

*All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.*⁵⁶

205. HIPAA applies to Defendant's webpages with tracking technologies even outside the password-protected patient account webpages:

Tracking on unauthenticated webpages

[T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking

⁵⁵ *Id.* (emphasis added).

⁵⁶ *Id.* (emphasis added).

technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity’s patient portal (which may be the website’s homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal ... **[and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances.** For example, tracking technologies could collect an individual’s email address and/or IP address when the individual visits a regulated entity’s webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.⁵⁷

206. This is further evidence that the data that Defendant chose to share is protected Personal Information. The sharing of that information was a violation of Class Members’ rights.

207. To be sure, the HHS Bulletin is not a pronouncement of new law, but instead reminded covered entities and business associates of their longstanding obligations under existing guidance. The Bulletin notes that “it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors,” then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.⁵⁸

208. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructed in 2012:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For

⁵⁷ *Id.* (emphasis added).

⁵⁸ *Id.* (citing, e.g., Modifications of the HIPAA [Rules], Final Rule, 78 FR 5566, 5598, a rulemaking notice from January 25, 2013, which stated: “[P]rotected health information ... may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected ... in accordance with the HIPAA rules.”).

instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.⁵⁹

209. In its guidance for Marketing, the Department further instructed in 2003:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.*⁶⁰

210. HHS has repeatedly instructed for years that patient status is protected by the HIPAA Privacy Rule:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002); and

It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013)

Plaintiffs and the Class Members did not consent to the interception and disclosure of their Private Information

⁵⁹ *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (November 26, 2012) at 5, available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coverentities/De-identification/hhs_deid_guidance.pdf (last visited Jun. 20, 2023).

⁶⁰ <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coverentities/marketing.pdf> (April 3, 2003) (emphasis added) (last visited Jun. 20, 2023).

211. Plaintiffs and Class Members had no idea when they interacted with Defendant’s websites that their personal data, including sensitive medical data, was being collected and simultaneously transmitted to Facebook. That is because, among other things, Meta Pixel is secretively and seamlessly integrated into Defendant’s websites and is invisible to patients visiting those websites.

212. For example, when Plaintiffs visited Defendant’s website in 2021, there was no indication that the Meta Pixel was embedded on that website or that it would collect and transmit their highly sensitive medical data to Facebook.

213. Plaintiffs and their fellow Class Members could not consent to Defendant’s conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook in the first place.

214. While Defendant purported to have a “Privacy Policy,” it gave no indication to patients that Defendant routinely allows Facebook to capture and exploit patients’ Private Information. Indeed, as of October 21, 2021 Defendant expressly promised that “We do not sell, trade, or otherwise transfer to outside parties your personal information unless we provide you with advance notice. This does not include website hosting partners and other parties who assist us in operating our Service, conducting our business, or servicing you, so long as those parties agree to keep this information confidential.”⁶¹

215. These statements were false, deceptive, and misleading because Defendant, in fact, tracked patients’ and potential patients’ IP addresses, cookies, and device identifiers, which it then caused the transmission of the same to third parties along with patients’ and potential patients’ sensitive medical information.

⁶¹ See The Internet Archive Wayback Machine, Workit Health, Inc. Privacy Policy (last revised August 30, 2021), available at <https://web.archive.org/web/20211021175816/https://www.workithealth.com/privacy-policy/>.

216. Defendant did not have a legal right to share Plaintiffs' and Class Members' PII/PHI without their written consent to third parties, because this information is protected from such disclosure by law. C.F.R. § 164.508. Nor was Defendant permitted to disclose patients' PII/PHI to advertising and marketing companies like Facebook without express written authorization from patients. 45 C.F.R. § 164.502(a)(5)(ii).

217. Defendant failed to obtain a valid written authorization from Plaintiffs or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications for marketing purposes.

218. Accordingly, Defendant lacked authorization to intercept, collect, and disclose Plaintiffs' and Class Members' PII/PHI to Facebook or aid in the same.

Plaintiffs' & Class Members' Reasonable Expectation of Privacy

219. At all times when Plaintiffs and Class Members provided their Private Information to Defendant, they each had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

220. Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information are grounded in, among other things, Defendant's status as a health care provider, Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

221. It was reasonable for Plaintiffs and Class Members to assume that Defendant's privacy policies were consistent with Defendant's duties to protect the confidentiality of patients' Private Information. The concern about sharing personal medical information is compounded by the reality that advertisers view this type of information as particularly valuable.

222. Many privacy law experts have expressed serious concerns about patients' sensitive medical information being disclosed to third-party companies like Facebook. As those critics have pointed out, having a patient's Private Information disseminated in ways the patient is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

Plaintiffs' & Class Members' Private Information Has Financial Value

223. Plaintiffs' and Class Members' Private Information has economic value.

224. Indeed, Facebook's, Google's and others' practices of using such information to package groups of people as "Lookalike Audiences" and similar groups and selling those packages to advertising clients demonstrates the financial worth of that data.

225. Data harvesting is the fastest growing industry in the nation. As software, data mining and targeting technologies have advanced, the revenue from digital ads and the consequent value of the data used to target them have risen rapidly.

226. Consumer data is so valuable that some have proclaimed that data is the new oil. Between 2016 and 2018, the value of information mined from Americans increased by 85% for Facebook and 40% for Google. Overall, the value internet companies derive from Americans' personal data increased almost 54%.

227. Conservative estimates suggest that in 2018, Internet companies earned \$202 per American user. In 2022, that value is expected to be \$200 billion industry wide, or \$434 per user, also a conservative estimate.

228. Tech companies are also under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own needs. For instance, the health data Google collects could eventually help it micro-target advertisements to people with particular health conditions. Policymakers are proactively calling for a revision and potential upgrade of the health privacy rules known as HIPAA, out of concern for what might happen as tech companies continue to march into the medical sector.⁶²

229. Time Magazine, similarly, in an article titled, How your Medical Data Fuels A Hidden Multi-Billion Dollar Industry, referenced the “growth of the big health data bazaar,” in which patients’ health information is sold. It reported that:

[T]he secondary market in information unrelated to a patient’s direct treatment poses growing risks, privacy experts say. That’s because clues in anonymized patient dossiers make it possible for outsiders to determine your identity, especially as computing power advances in the future.⁶³

230. Workit gave away Plaintiff’s and Class Members’ communications and transactions on its Website without prior, informed consent.

231. The unauthorized access to and dissemination of Plaintiffs’ and Class Members’ private and Private Information has diminished the value of that information, resulting in harm to Defendant’s Users.

⁶² CNBC, HOSPITAL EXECs SAY THEY ARE GETTING FLOODED WITH REQUESTS FOR YOUR HEALTH DATA, <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-withrequests-for-your-health-data.html> (last visited May 8, 2023).

⁶³ Time, HOW YOUR MEDICAL DATA FUELS A HIDDEN MULTI-BILLION DOLLAR INDUSTRY, <https://time.com/4588104/medical-data-industry/> (last visited May 22, 2023).

Defendant Was Unjustly Enriched & Benefitted from the Use of The Pixel, Google Analytics, & Its Unauthorized Disclosures.

232. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiffs' and class members' Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing the personally identifiable information of its patients, Defendant is compensated by Facebook and/or Google in the form of enhanced advertising services and more cost-efficient marketing on Facebook and/or Google.

233. Upon information and belief, Defendant was advertising its services on Facebook, and the Pixel was used to help Defendant understand the success of its advertisement efforts on Facebook.

234. Retargeting is a form of online marketing that targets users with ads based on their previous Internet communications and interactions.

235. Upon information and belief, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so through use of the intercepted patient data in the absence of express written consent.

236. By utilizing the Pixel and/or Google Analytics, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiffs and Class Members.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

Plaintiff Jane Doe 1

237. Plaintiff Jane Doe 1 first used Defendant's Website on or about April 2, 2021 for the purpose of seeking and obtaining substance use services.

238. Plaintiff accessed Defendant's Website to receive services from Defendant at Defendant's direction.

239. As a condition of seeking and receiving Defendant's services, Plaintiff input Private Information into Defendant's Website on multiple occasions, including information about her substance abuse history, her condition and treatments, requests for substance use services, and other information as prompted to obtain substance use services.

240. Plaintiff was a patient of Defendant's and received substance use services from Defendant.

241. Plaintiff provided Private Information to Defendant through its Website on multiple occasions.

242. Plaintiff used the same devices to maintain and access Defendant's Website, and she was an active Facebook user who used the same devices to access Facebook.

243. Plaintiff's communications with Defendant were for the purpose of seeking and obtaining substance use treatment, and she believed that those communications would be kept private and not be disclosed to any third party.

244. Plaintiff reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

245. Plaintiff paid Defendant for the services she received.

246. Plaintiff's use of Defendant's Website constitutes communications between Plaintiff and Defendant. Those communications were transmitted and passed over a wire, cable, or other like connection.

247. Plaintiff is a Facebook user, had a Facebook account at all times that she used Defendant's Website, and was logged into her Facebook account at all times while using Defendant's Website.

248. Plaintiff's Facebook profile contains her name, whereby she can be personally identified by that information.

249. After Plaintiff provided information to Defendant through its Website, Plaintiff started receiving numerous advertisements through her Facebook page relating to substance abuse services. These advertisements included advertisements from Workit. She has noticed changes in the quantity and content of the advertisements since she provided Private Information to Defendant. These advertisements included solicitations for mental health and substance abuse services. Plaintiff still received ads after she stopped using Workit's websites and discontinued receiving services from Workit. The ads have increased since she stopped seeking and receiving services from Workit.

250. Facebook is not a party to the communications between Plaintiff and Defendant.

251. Upon information and belief, each time Plaintiff used Defendant's Website, Defendant willfully disclosed Plaintiff's FID, along with the Private Information she entered.

252. This simultaneous disclosure of information allowed Facebook to read or learn the contents of communications between Plaintiff and Defendant.

253. Google is not a party to the communications between Plaintiff and Defendant.

254. Upon information and belief, each time Plaintiff used Defendant's Website, Defendant willfully disclosed Plaintiff's IP address and other personally identifying information along with the information she entered for the purpose of seeking and obtaining substance use treatment to Google via Google Analytics.

255. This simultaneous disclosure of information allowed Google to read or learn the contents of communications between Plaintiff and Defendant.

256. As described herein, Defendant worked along with Facebook and Google to willfully disclose, intercept, use, and facilitate the interception of her private communications regarding Plaintiff's private medical information without Plaintiff's knowledge, informed consent, or express written authorization.

257. Defendant intentionally allowed Facebook and Google to secretly intercept communications between Plaintiff and Defendant about Plaintiff's private medical information.

258. Plaintiff did not know that communications between her and Defendant would be disclosed to, or intercepted by, Facebook and Google.

259. Plaintiff did not know that her medical information would be used by Defendant for any purpose other than providing medical services.

260. Plaintiff did not, and does not, consent to communications between her and Defendant being disclosed to Facebook, Google, or any other third party.

261. Defendant did not seek Plaintiff's prior, informed consent before disclosing her Private Information to third parties.

262. Plaintiff did not authorize the sharing, selling, or use of her medical information.

263. Upon information and belief, Defendant intentionally, willfully, and surreptitiously disclosed private and confidential communications between Plaintiff and Defendant to third parties, including Facebook and Google, for profit.

264. Plaintiff suffered an injury and/or damages in the form of (i) invasion of privacy; (ii) being subjected to unsolicited and unwanted advertisements targeting her because of Defendant's unlawful conduct; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; and (v) nominal damages; (vi) punitive damages; and/or (vii) statutory damages.

Plaintiff Jane Doe 2

265. Plaintiff Jane Doe 2 first used Defendant's Website on or about October 2021 for the purpose of seeking and obtaining substance use services.

266. Plaintiff accessed Defendant's Website to receive services from Defendant at Defendant's direction.

267. As a condition of seeking and receiving Defendant's services, Plaintiff input Private Information into Defendant's Website, including by filling out Defendant's intake form and providing information about her medical condition, requests for substance use services, and other information as prompted to obtain substance use services.

268. Plaintiff was a patient of Defendant's and received substance use services from Defendant, including seeing a coach and doctors.

269. Plaintiff provided Private Information to Defendant through its Website on multiple occasions.

270. Plaintiff was an active Facebook user who used the same devices to access her private Facebook page.

271. Plaintiff's communications with Defendant were for the purpose of seeking and obtaining substance use treatment, and she believed that those communications would be kept private and not be disclosed to any third party.

272. Plaintiff reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant and that such communications would not be transmitted to or intercepted by a third party.

273. Plaintiff paid Defendant for the services she received.

274. Plaintiff's use of Defendant's Website constitutes communications between Plaintiff and Defendant. Those communications were transmitted and passed over a wire, cable, or other like connection.

275. Plaintiff's Facebook profile contains her name, whereby she can be personally identified by that information.

276. After Plaintiff provided information to Defendant through its Website, Plaintiff received numerous advertisements through Facebook relating to substance abuse services. Plaintiff noticed changes in the quantity and content of the advertisements through Facebook since she provided Private Information to Defendant and even tried to clear her cookies to stop the advertisements.

277. Facebook is not a party to the communications between Plaintiff and Defendant.

278. Upon information and belief, each time Plaintiff used Defendant's Website, Defendant willfully disclosed Plaintiff's FID, along with the Private Information she entered.

279. This simultaneous disclosure of information allowed Facebook to read or learn the contents of communications between Plaintiff and Defendant.

280. Google is not a party to the communications between Plaintiff and Defendant.

281. Upon information and belief, each time Plaintiff used Defendant's Website, Defendant willfully disclosed Plaintiff's IP address and/or other personally identifying information along with the information she entered for the purpose of seeking and obtaining substance use treatment to Google via Google Analytics.

282. This simultaneous disclosure of information allowed Google to read or learn the contents of communications between Plaintiff and Defendant.

283. As described herein, Defendant worked along with Facebook and Google to willfully disclose, intercept, use, and facilitate the interception of her private communications regarding Plaintiff's private medical information without Plaintiff's knowledge, consent, or express written authorization.

284. Defendant intentionally allowed Facebook and Google to secretly intercept communications between Plaintiff and Defendant about Plaintiff's private medical information.

285. Plaintiff did not know that communications between her and Defendant would be disclosed to, or intercepted by, Facebook and Google.

286. Plaintiff did not know that her medical information would be used by Defendant for any purpose other than providing medical services.

287. Plaintiff did not, and does not, consent to communications between her and Defendant being disclosed to Facebook, Google, or any other third party.

288. Defendant did not seek Plaintiff's prior, informed consent before disclosing her Private Information to third parties.

289. Plaintiff did not authorize the sharing, selling, or use of her medical information.

290. Upon information and belief, Defendant intentionally, willfully, and surreptitiously disclosed private and confidential communications between Plaintiff and Defendant to third parties, including Facebook and Google, for profit.

291. Plaintiff suffered an injury and/or damages in the form of (i) invasion of privacy; (ii) being subjected to unsolicited and unwanted advertisements targeting her because of Defendant's unlawful conduct; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; and (v) nominal damages; (vi) punitive damages; and/or (vii) statutory damages.

TOLLING

292. Any applicable statute of limitations has been tolled by the discovery rule. Plaintiffs did not know (and had no way of knowing) that Plaintiffs' private information was intercepted and unlawfully disclosed because Defendant kept this information secret.

CLASS ALLEGATIONS

A. Definition of the Class

293. Plaintiffs bring this action individually and on behalf of all persons that the Court may determine appropriate for class certification, pursuant to Fed. R. Civ. P. 23 (the "Class").⁶⁴ Plaintiffs seek to represent a "Nationwide Class" of persons preliminarily defined as:

All persons who have a Facebook account and used Defendant's Website to search for medical information, services or physicians, schedule appointments, register for programs or support groups, or pay for medical services.

Additionally, Plaintiffs seek to represent a "California Sub-Class" of persons preliminarily defined as:

⁶⁴ Plaintiffs allege that certification is proper under both Fed. R. Civ. P. 23(b)(2) and 23(b)(3).

All persons in California who have a Facebook account and used Defendant's Website to search for medical information, services or physicians, schedule appointments, register for programs or support groups, or pay for medical services.

These class definitions are subject to modification as discovery discloses further information.

Plaintiffs reserve the right to propose one or more additional sub-classes if discovery reveals that such subclasses are appropriate.

294. This case is properly maintainable as a class action pursuant to and in accordance with Fed. R. Civ. P. 23 in that:

- a) The Class, which includes thousands of members, is so numerous that joinder of all Class Members is impracticable;
- b) There are substantial questions of law and fact common to the Class, including those set forth in greater particularity herein;
- c) Questions of law and fact, such as those enumerated below, which are common to the Class, predominate over any questions of law or fact affecting only individual members of the Class;
- d) The claims of the representative party are typical of the claims of the Class;
- e) A class action is superior to any other type of action for the fair and efficient adjudication of the controversy;
- f) The relief sought in this class action will effectively and efficiently provide relief to all members of the Class;
- g) There are no unusual difficulties foreseen in the management of this class action; and
- h) Plaintiffs, whose claims are typical of those of the Class, through their experienced counsel, will zealously and adequately represent the Class.

B. Numerosity

295. There are thousands of individuals who have used Defendant's Website to communicate medical information, seek services or physicians, schedule appointments, register for programs or support groups, or pay for medical services. Accordingly, the Class Members are so numerous that joinder of all parties is clearly impracticable.

296. The prosecution of separate lawsuits by Class Members would risk inconsistent or varying adjudications. Class-wide adjudication of these claims is, therefore, appropriate.

C. Commonality

297. Numerous common questions of law and fact predominate over any questions affecting individual Class Members including, but not limited to, the following:

- a) Whether Defendant collected information about Class Members who used its Website;
- b) Whether Defendant disclosed communications between Defendant and Class Members via Facebook Pixel and/or similar tools;
- c) Whether such disclosures were willful or intentional;
- d) Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;
- e) Whether Defendant violated its privacy policy and/or applicable law by disclosing Private Information of Plaintiffs and Class Members to Facebook, Google, and/or additional third parties;
- f) Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to Third Parties;
- g) Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;
- h) Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

- i) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;
- j) Whether Defendant violated the Michigan Consumer Protection Act;
- k) Whether Plaintiffs' Private Information constitutes messages, reports, or communications under section 631 of the CIPA;
- l) Whether Plaintiffs' Private Information constitutes medical information under section 56.10(d) of the CMIA;
- m) Whether Plaintiffs are entitled to actual, consequential, nominal, statutory, or punitive damages as a result of Defendant's wrongful conduct;
- n) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information;
- o) Whether Defendant shared, sold, or used Class Members' Private Information for purposes other than providing healthcare services;
- p) Whether such disclosure was willful, intentional, or negligent;
- q) The nature and extent of messages, reports, communications, and medical information disclosed;
- r) How Class Members' messages, reports, communications, and medical information were disclosed and to whom; and
- s) Whether Defendant's Website obtained consent or authorization before disclosing Class Members' Private Information.

D. Typicality

298. Plaintiffs have the same interests in this matter as all other members of the Class and their claims are typical of the claims of all members of the Class. If brought and prosecuted individually, the claims of each Class Member would require proof of substantially the same material and substantive facts, utilize the same complex evidence (e.g. expert testimony), rely upon the same legal theories, and seek the same type of relief.

299. The claims of Plaintiffs' and other Class Members have a common cause and their damages are of the same type.

300. The claims originate from the synonymous disclosure of Private Information or communications by Defendant without prior, informed consent.

301. All Class Members have been aggrieved by Defendant's disclosure of their Private Information or communications by Defendant without prior, informed consent.

E. Adequacy of Representation

302. Plaintiffs' claims are sufficiently aligned with the interests of the absent Class Members to ensure that the Class' claims will be prosecuted with diligence and care by Plaintiffs as representative of the Class. Plaintiffs will fairly and adequately represent the interests of the Class and they do not have interests adverse to the Class.

303. Plaintiffs have retained the services of counsel who are experienced in complex class action litigation. Plaintiffs' counsel will vigorously prosecute this action and will otherwise protect and fairly and adequately represent the Plaintiffs and all absent Class Members.

F. Superiority

304. A class action is superior to other methods for the fair and efficient adjudication of the controversies raised in this Complaint because:

- a) Individual claims by the Class Members would be impracticable as the costs of pursuit would far exceed what any one Class Member has at stake;
- b) Individual claims by Class Members would create a risk of inconsistent or varying adjudications, which would present the Defendant with incompatible standards of conduct;
- c) Individual claims by individual Class Members would create a risk of adjudications which would, as a practical matter, be dispositive of the interests of other individuals who are not parties to the

adjudications, or substantially impair or impede their ability to protect and pursue their interests;

- d) Little or no individual litigation has been commenced over the controversies alleged in this Complaint and individual Class Members are unlikely to have an interest in separately prosecuting and controlling individual actions;
- e) In view of the complexity of the issues and the expenses of litigation, the separate claims of individual Class Members are likely insufficient in amount to support the costs of filing and litigating separate actions;
- f) Plaintiff seeks relief relating to the Defendant's common actions and the equitable relief sought would commonly benefit the Class as a whole;
- g) The concentration of litigation of these claims in one action will achieve efficiency and promote judicial economy; and
- h) The proposed class action is manageable.

305. Additionally, Defendant has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

CLAIMS

COUNT I

Invasion of Privacy – Intrusion Upon Seclusion and Private Affairs *(On Behalf of Plaintiffs & the Class)*

306. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

307. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

308. The Private Information of Plaintiffs and Class Members consists of private and confidential facts and information, including protected identifying information and protected

health information protected by HIPAA, that were never intended to be shared beyond Plaintiffs' private communications with Defendant relating to substance use disorder services.

309. Plaintiffs and Class Members have a right to have their Private Information protected from unauthorized acquisition without their expressed, written consent. See MCL § 330.1262; MCL § 330.1263. Matters concerning a person's medical treatment or condition are generally considered private.

310. Michigan Law provides with respect to Substance Use Disorder Services, which Defendant advertises and offers through its website and mobile app, that "Records of the identity, diagnosis, prognosis, and treatment of an individual maintained in connection with the performance of a program, an approved service program, or an emergency medical service authorized or provided or assisted under this chapter are confidential[.]" MCL § 330.1261.

311. Michigan Law further provides with respect to Substance Use Disorder Services, which Defendant advertises and offers through its website and mobile app, that "Records of the diagnostic evaluation, psychiatric, psychological, social service care, and referral of an individual that are maintained in connection with the performance of an approved service program ... are confidential[.]" MCL § 330.1285.

312. Unless an individual seeking substance use disorder services provides express written consent authorizing disclosure, such Private Information relating to Substance Use Disorder Services may only be acquired for the purpose of the program for which it is solicited, "the diagnosis and treatment of individuals with a substance use disorder" and "to provide substance use disorder services." MCL § 330.1260(1)(c); MCL § 330.1260(1)(i).

313. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy regarding their private information and were accordingly entitled to the protection of this information against secret, unauthorized acquisition and/or disclosure to third parties.

314. In addition, Plaintiffs and Class Members have a reasonable expectation that Defendant will not place tracking devices on its own patients' communications devices without their knowledge or informed consent.

315. The information Plaintiffs and Class Members shared with Defendant was of a personal, intimate, and/or embarrassing nature, and/or was otherwise protected from unauthorized acquisition and/or disclosure by law, including HIPAA and Michigan Law.

316. Defendant, a health care provider, owed a duty to Plaintiffs and Class Members to keep their personally identifiable patient data, communications, and private information secure and confidential and not to acquire it for other purposes without express written consent.

317. The secret and unauthorized acquisition and/or disclosure of Plaintiffs' and Class Members' private information via Defendant's utilization of the Tracking Pixel and/or Google Analytics is highly offensive to a reasonable person.

318. When Plaintiffs and Class Members provided private information to Defendant, Defendant failed to notify them that it was secretly using the Tracking Pixel and/or Google Analytics to simultaneously acquire this information for commercial purposes entirely unrelated to registration, clinical care, diagnosis, or treatment.

319. In fact, Defendant expressly promised to maintain the confidentiality of personally identifiable patient data and communications. Defendant's website boasts that "Workit Health's web app, mobile app, and electronic medical records system are HIPAA compliant."⁶⁵

⁶⁵ <https://www.workithealth.com/accreditations-and-experts/> (last visited June 27, 2023).

Security and Accessibility

HIPAA Compliant

Workit Health's web app, mobile app, and electronic medical records system are HIPAA compliant.

SOC 2 Type II Certified

Workit Health's electronic medical records system is SOC 2 Type II certified.

320. Defendant failed to notify Plaintiffs and Class Members that it was utilizing concealed tracking technology that was simultaneously, and for purposes unrelated to substance use disorder services, acquiring their private information for transmission to Facebook, Google, and other third parties for Defendant's own commercial purposes, including Defendant's own advertising advantages. To the contrary, Defendant affirmatively and prominently promised Plaintiffs and the Class before they provided any information that "All of the information you share is kept private and is protected by our HIPAA-compliant software."⁶⁶

⁶⁶ <https://app.workithealth.com/signup> (last visited June 27, 2023).

Sign up for Workit Health

Get started by answering a few questions to help us determine which program is right for you. All of the information you share is kept private and is protected by our HIPAA-compliant software.

Continue

321. After Workit users click on the “Continue” button to sign up with Defendant, the “Start your Workit profile” page once again assures users that “We take your privacy seriously. Your information is protected by our HIPAA compliant software.” Defendant’s statement prominently encourages users to provide personal and admittedly HIPAA-protected information to Defendant prior to signing up, with assurances that the private information they provide will be kept private.⁶⁷

⁶⁷ https://app.workithealth.com/onboarding/zip_code (last visited June 27, 2023).

Start your Workit profile

First Name (Preferred) (Required)

Date of Birth (Required)

ZIP/Postal Code (Required)

How did you hear about us? (Required)

Continue

We take privacy seriously. Your information is protected by our HIPAA compliant software. [Learn more about our privacy practices.](#)

Already scheduled an appointment over the phone? [Activate account](#)

Already have an account? [Sign in](#)

322. Defendant failed to provide Plaintiffs and Class Members an opportunity to give signed, written consent to Defendant to acquire their Private Information through the surreptitious use of tracking technologies, and Plaintiffs did not otherwise authorize or consent to Defendant's acquisition of their Private Information for purposes outside of program registration, diagnosis, medical advice, care, and/or treatment of a substance use disorder service.

323. Defendant's methodology of employing a secret and unauthorized use of tracking technology to acquire Plaintiffs' personally identifiable patient data for purposes entirely unrelated

to program registration, diagnosis, medical advice, care, and/or treatment of a substance use disorder service and communications is objectionable to Plaintiffs.

324. Defendant's affirmative promises to keep all information shared through Defendant's website private and protected from third-party acquisition and disclosure was knowingly false and without authorization.

325. Defendant's knowing, willful, and intentional acquisition of Plaintiffs' and Class Members' private information constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude, seclusion, and privacy of their private affairs. Defendant's secret and undisclosed acquisition of Plaintiffs' and Class Members' Private Information by Tracking Pixel technology is, and would be, highly offensive to a reasonable person.

326. Defendant's acts violated its legal duties, in addition to its common law standard of care. In June 2022, a publication called The Markup reported that "Facebook is Receiving Sensitive Medical Information from Hospital Websites." The article quoted numerous experts, none of which defended the practice of hospitals incorporating such tools onto their properties.

- a. David Holtzman, described as a "health privacy consultant who previously served as a senior privacy advisor in the U.S. Department of Health and Human Services' Office of Civil Rights" and whose LinkedIn profile states that he served as a consultant for "healthcare organizations in defense of claims or regulatory actions alleging inadequate information privacy and security standards," stated: (1) "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it. I cannot say [sharing this data] is for certain a HIPAA violation. It is quite likely a HIPAA

violation.”; and (2) “When an individual has sought out a provider and indicated that they want to make an appointment, at that point, any individually identifiable health information that they’ve provided in this session, in the past, or certainly in the future, is protected under HIPAA and could not be shared with a third party like Facebook.”

- b. Iliana Peters, described as “a privacy lawyer with the firm Polsinelli who previously headed HIPAA enforcement for the Office for Civil Rights,” stated, “Generally, HIPAA covered entities and business associates should not be sharing identifiable information with social media companies unless they have HIPAA authorization [from the individual] and consent under state law.”
- c. Glenn Cohen, described as the “faculty director of Harvard Law School’s Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics,” stated, “Almost any patient would be shocked to find out that Facebook is being provided an easy way to associate their prescriptions with their name. Even if perhaps there’s something in the legal architecture that permits this to be lawful, it’s totally outside the expectations of what patients think the health privacy laws are doing for them.”

327. State and federal judges have expressed similar sentiments, finding similar allegations stated privacy claims that require conduct that would be considered “highly offensive” to a reasonable person. *See, e.g., In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO,

2022 WL 17869218 (N.D. Cal. Dec. 22, 2022); *Doe v. Bon Secours Mercy Health*, No. A 2002633, 2021 WL 9939010, at *4-5 (Ohio C.P. Nov. 22, 2021) (declining to dismiss invasion of privacy claim against hospital that implemented Facebook Pixel on website); *Doe v. Virginia Mason*, 2020 WL 1983046, at *2 (Wash. Super. Feb. 12, 2020); *Doe v. Medstar*, Case No. 24-C-20-000591 (Baltimore City, Maryland); and *Doe v. Partners*, Case No. 1984-CV-01651 (Suffolk County, Massachusetts).

328. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when it incorporated tracking technologies into its Website because it knew the functionality and purpose of the Tracking Pixel and/or Google Analytics.

329. Because Defendant intentionally and willfully incorporated tracking technologies into its Website and encouraged patients to use that Website for healthcare purposes, while untruthfully promising that "All of the information you share is kept private and is protected by our HIPAA-compliant software", Defendant had actual knowledge that its practices would cause injury to Plaintiffs and Class Members.

330. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiffs and Class Members was wrongfully acquired, for impermissible and unauthorized purposes, and without authorized written consent, causing Plaintiffs and the Class to suffer an injury to their privacy, seclusion, and security in their private affairs.

331. These injuries were exacerbated by Defendant's subsequent disclosure of the information to third parties for commercial purposes for which Plaintiffs received no benefit and for which they did not provide signed, written consent.

332. Defendant's intentional, willful and reckless conduct in secretly acquiring Plaintiffs' and Class Members' Private Information and communications for secret and

unauthorized purposes caused serious mental injury to Plaintiffs and Class Members, including shame and/or humiliation.

333. Plaintiffs and Class Members have suffered injuries and damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Defendant intruded upon, acquired, intercepted, transmitted, shared, and used their individually identifiable patient health information (including information about their medical symptoms, conditions and concerns, medical appointments, healthcare providers and locations, medications and treatments and health insurance and medical bills) for impermissible and previously undisclosed commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;
- b. Plaintiffs suffered a loss of confidentiality in private and legally protected Private Information for undisclosed and impermissible purposes;
- c. Plaintiffs suffered a loss of privacy as a result of Defendant's unlawful acquisition of their private information for undisclosed and impermissible purposes;
- d. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' individually identifiable patient health information without providing any value or benefit to Plaintiffs or the Class Members;

- e. Defendant received substantial and quantifiable value from its use of Plaintiffs' and the Class Members' individually identifiable patient health information, such as understanding how people use its Website and determining what ads people see on its Website, without providing any value or benefit to Plaintiffs or the Class Members;
- f. Plaintiffs lost value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;
- g. Plaintiffs were subjected to unwanted advertisements by Defendant and/or third parties as a result of Defendant's violation of their privacy and confidentiality;
- h. Diminished value of Plaintiffs' PII and PHI;⁶⁸

⁶⁸ Numerous courts have recognized that plaintiffs whose personal information is unlawfully disclosed have suffered an economic injury. *See, e.g., Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021) (“[T]he Ninth Circuit and a number of district courts, including this Court, have concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had standing.”); *In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020) (“[T]he growing trend across courts that have considered this issue is to recognize the lost property value of this information.”); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (holding that plaintiffs had adequately alleged injury in fact based on the loss of value of their personal information); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *14 (N.D. Cal. May 17, 2016) (concluding that the plaintiffs had plausibly alleged injury from the loss of value of their personal information); *Smallman v MGM Resorts Int’l*, 2:20-cv-00376-GMN-EJY, 2022 WL 16636958, at *6 (D. Nev. Nov. 2, 2022) (personal information can be bought and sold at identifiable prices in established markets and therefore has value; disclosure of personal information constitutes harm for injury in fact purposes).

- i. General damages for invasions of privacy and confidentiality rights;
- j. Nominal damages; and
- k. Punitive damages.

334. Plaintiffs, on behalf of themselves and the Class, seek nominal, compensatory, and punitive damages for Defendant's invasions of their privacy.

335. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their Private Information is still maintained by Defendant and still in the possession of Facebook, Google and/or other third parties, and the wrongful acquisition and disclosure of the information cannot be undone.

336. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook and/or Google, who on information and belief continues to possess and utilize that information.

337. Plaintiffs, on behalf of themselves and Class Members further seek declaratory and injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II

**Invasion of Privacy – Public Disclosure of Embarrassing Private Facts
(On Behalf of Plaintiffs & the Class)**

338. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

339. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

340. Plaintiffs' and Class Members' communications with Defendant constitute private conversations, matters, facts, and data.

341. The private information of Plaintiffs and Class Members provided in confidence to Defendant consists of private and confidential facts and information, including protected identifying information (PII) and protected health information (PHI) protected by HIPAA and Michigan Law, that were never intended to be shared beyond Plaintiffs' private communications with Defendant relating to substance use disorder services.

342. Plaintiffs and Class Members have a right to have their Private Information protected from unauthorized disclosure without their expressed, written consent. See MCL § 330.1262; MCL § 330.1263. Matters concerning a person's medical treatment or condition are generally considered private and are protected by law, including HIPAA.

343. Michigan Law provides with respect to Substance Use Disorder Services, which Defendant advertises and offers through its website and mobile app, that "Records of the identity, diagnosis, prognosis, and treatment of an individual maintained in connection with the performance of a program, an approved service program, or an emergency medical service authorized or provided or assisted under this chapter are confidential[.]" MCL § 330.1261.

344. Michigan Law further provides with respect to Substance Use Disorder Services, which Defendant advertises and offers through its website and mobile app, that “Records of the diagnostic evaluation, psychiatric, psychological, social service care, and referral of an individual that are maintained in connection with the performance of an approved service program ... are confidential[.]” MCL § 330.1285.

345. Unless an individual seeking substance use disorder services provides express written consent authorizing disclosure, such Private Information relating to Substance Use Disorder Services may only be disclosed for specific enumerated purposes, none of which apply here. *See* MCL § 330.1262; MCL § 330.1263. Michigan Law does not allow for disclosure of confidential information relating to Substance Use Disorder Services for Defendant’s private commercial purposes, including advertising or as a private revenue source, without a patient’s express, written consent.

346. Plaintiffs and Class Members have a reasonable expectation that Defendant would not disclose personally identifiable patient data and communications to third parties for marketing purposes without Plaintiffs’ and other Class Members’ authorization, consent, knowledge, or any further action on the patient’s part.

347. In addition, Plaintiffs and Class Members have a reasonable expectation that Defendant will not place tracking devices on its own patients’ communications devices without their knowledge or prior, informed consent.

348. The information Plaintiffs and Class Members shared with Defendant was of a personal, intimate, and/or embarrassing nature, and was protected from unauthorized disclosure by law, including MCL § 330.126, MCL § 330.1285, and HIPAA.

349. Defendant, a health care provider, owed a duty to Plaintiffs and Class Members to keep their personally identifiable patient data, communications, and private information secure and confidential and not to disclose or sell it without express written consent.

350. The secret and unauthorized disclosure of Plaintiffs' and Class Members' private information to major online service providers with an expansive reach into the public sphere, like Facebook and Google, via Defendant's utilization of surreptitious tracking technology is highly offensive to a reasonable person.

351. Defendant unlawfully published Plaintiffs' and class Members' private facts by deploying source code that caused the transmission of Plaintiffs' Class Members' PII, PHI, and the contents of communications Plaintiffs and Class Members exchanged with their health care providers to third parties, including Facebook and Google.

352. Plaintiffs and Class Members did not authorize, consent to, know about, or take any action to indicate consent to Defendant's conduct alleged herein.

353. When Plaintiffs and Class Members provided private information to Defendant, Defendant failed to notify them that it was secretly using the Tracking Pixel and/or Google Analytics to simultaneously acquire this information for commercial purposes entirely unrelated to registration, clinical care, diagnosis, or treatment.

354. In fact, Defendant expressly promised to maintain the confidentiality of personally identifiable patient data and communications. Defendant's website boasts that "Workit Health's web app, mobile app, and electronic medical records system are HIPAA compliant."⁶⁹

⁶⁹ <https://www.workithealth.com/accreditations-and-experts/> (last visited June 27, 2023).

Security and Accessibility

HIPAA Compliant

Workit Health's web app, mobile app, and electronic medical records system are HIPAA compliant.

SOC 2 Type II Certified

Workit Health's electronic medical records system is SOC 2 Type II certified.

355. Defendant failed to notify Plaintiffs and Class Members that it was utilizing concealed tracking technologies that were simultaneously, and for purposes unrelated to substance use disorder services, acquiring their private information for transmission to Facebook, Google, and other third parties for Defendant's own commercial purposes, including Defendant's own advertising advantages. To the contrary, Defendant affirmatively and prominently promised Plaintiffs and the Class before they provided any information that "All of the information you share is kept private and is protected by our HIPAA-compliant software."⁷⁰

⁷⁰ <https://app.workithealth.com/signup> (last visited June 27, 2023).

Sign up for Workit Health

Get started by answering a few questions to help us determine which program is right for you. All of the information you share is kept private and is protected by our HIPAA-compliant software.

Continue

356. After Workit users click on the “Continue” button to sign up with Defendant, the “Start your Workit profile” page once again assures users that “We take your privacy seriously. Your information is protected by our HIPAA compliant software.” Defendant’s statement prominently encourages users to provide personal and admittedly HIPAA-protected information to Defendant prior to signing up, with assurances that the private information they provide will be kept private.⁷¹

⁷¹ https://app.workithealth.com/onboarding/zip_code (last visited June 27, 2023).

Start your Workit profile

First Name (Preferred) (Required)

Date of Birth (Required)

ZIP/Postal Code (Required)

How did you hear about us? (Required)

Continue

We take privacy seriously. Your information is protected by our HIPAA compliant software. [Learn more about our privacy practices.](#)

Already scheduled an appointment over the phone? [Activate account](#)

Already have an account? [Sign in](#)

357. Defendant failed to provide Plaintiffs and Class Members an opportunity to give signed, written consent to Defendant to acquire their Private Information through the Tracking Pixel and/or Google Analytics, and Plaintiffs did not otherwise authorize or consent to Defendant's acquisition of their Private Information for purposes outside of program registration, diagnosis, medical advice, care, and/or treatment of a substance use disorder service.

358. Plaintiffs' and Class Members' Private Information and communications are the type of sensitive, Private Information that one normally expects will be protected from disclosure

to unauthorized parties by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and Class Members' Private Information and communications, and such information is otherwise protected from exposure to the public by the statutes, regulations, and laws described herein.

359. Defendant's methodology of employing a secret and unauthorized use of tracking technologies to acquire and secretly disclose Plaintiffs' personally identifiable patient data for purposes entirely unrelated to program registration, diagnosis, medical advice, care, and/or treatment of a substance use disorder service and communications is objectionable to Plaintiffs.

360. Defendant's affirmative promises to keep all information shared through Defendant's website private and protected from third-party acquisition and disclosure was knowingly false and without authorization.

361. Defendant's conduct was knowing and intentional as shown by its decision to install the Pixel and/or Google Analytics onto its Website.

362. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when it incorporated surreptitious tracking technologies into its Website because it knew the functionality and purpose of the Tracking Pixel, which sends information to Facebook via scripts running in an internet browser and links it to data that can be used to identify the individual or household associated with the information. The Tracking Pixel also commonly links to third-party cookies—another tracking mechanism—that allow Facebook to link the data to specific user accounts. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

363. Defendant's disclosure of Plaintiffs' Private Information—which likely included answers to medical questionnaires, name, email address, phone number, as well as information

about medical products they may have purchased on Workit’s website – has been sent to advertising platforms, along with the information needed to identify Plaintiffs and Class Member users. Such data is highly personal and can be used to target advertisements for services that may be unnecessary or that may be “potentially harmful physically, psychologically, or emotionally.”⁷²

364. Plaintiffs have had active Facebook accounts during the relevant time period and, following Defendant’s disclosures, they suddenly started to receive unsolicited advertisements relating to Workit and various addiction treatments shortly after signing up for Workit services, even after ending the use of the Workit website. Defendant’s disclosures were given publicity that has become, or is substantially certain to become, public knowledge.

365. Plaintiffs’ Private Information was not a matter of public record or otherwise open to the public at the time of Defendant’s wrongful disclosure.

366. Defendant’s disclosure of Plaintiffs’ Private Information caused unreasonable publicity of Plaintiffs’ highly sensitive private facts.

367. Defendant’s knowing, willful, and intentional disclosure of Plaintiffs’ and Class Members’ private information constitutes an intentional interference with Plaintiffs’ and Class Members’ interest in solitude, seclusion, and privacy of their private affairs. Defendant’s secret and unauthorized disclosure of Plaintiffs’ and Class Members’ Private Information by the use of surreptitious tracking technology is, and would be, highly offensive to a reasonable person.

368. Because Defendant intentionally and willfully incorporated tracking technologies into its Website and encouraged patients to use that Website for healthcare purposes, while untruthfully promising that “All of the information you share is kept private and is protected by

⁷² See <https://www.commerce.senate.gov/2023/2/cantwell-klobuchar-collins-lummis-call-on-telehealth-companies-to-protect-patients-sensitive-health-data> (last visited June 27, 2023).

our HIPAA-compliant software”, Defendant had actual knowledge that its practices would cause widespread disclosure of Plaintiffs’ private information and cause injury to Plaintiffs and Class Members.

369. As a proximate result of Defendant’s acts and omissions, the private and sensitive PII and PHI of Plaintiffs and Class Members was wrongfully acquired and disclosed, for impermissible and unauthorized purposes, and without prior, written consent or authorization, causing Plaintiffs and the Class to suffer an injury to their privacy, seclusion, and security in their private affairs.

370. Defendant’s intentional, willful and reckless conduct in secretly acquiring and disclosing Plaintiffs’ and Class Members’ Private Information and communications to the public caused serious mental injury to Plaintiffs and Class Members, including shame and/or humiliation and caused them to be repeatedly subjected to unsolicited advertisements.

371. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant’s invasion of privacy in that:

- a. Defendant intruded upon, acquired, intercepted, transmitted, shared, and used their individually identifiable patient health information (including information about their medical symptoms, conditions and concerns, medical appointments, healthcare providers and locations, medications and treatments and health insurance and medical bills) for impermissible and previously undisclosed commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;

- b. Plaintiffs suffered a loss of confidentiality in private and legally protected Private Information for undisclosed and impermissible purposes;
- c. Plaintiffs suffered a loss of privacy as a result of Defendant's unlawful acquisition of their private information for undisclosed and impermissible purposes;
- d. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' individually identifiable patient health information without providing any value or benefit to Plaintiffs or the Class Members;
- e. Defendant received substantial and quantifiable value from its use of Plaintiffs' and the Class Members' individually identifiable patient health information, such as understanding how people use its Website and determining what ads people see on its Website, without providing any value or benefit to Plaintiffs or the Class Members;
- f. Plaintiffs lost value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;
- g. Plaintiffs were subjected to unwanted advertisements by Defendant and/or third parties as a result of Defendant's violation of their privacy and confidentiality;
- h. Diminished value of Plaintiffs' PII and PHI;

- i. General damages for invasions of privacy and confidentiality rights;
- j. Nominal damages; and
- k. Punitive damages.

372. Plaintiffs, on behalf of themselves and the Class, seek nominal, compensatory, and punitive damages for Defendant's invasions of their privacy.

373. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their Private Information is still maintained by Defendant and still in the possession of Facebook, Google and/or other third parties, and the wrongful disclosure of the information cannot be undone.

374. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook, Google, and third-party advertisers who on information and belief continues to possess and utilize that information.

375. Plaintiffs, on behalf of themselves and Class Members further seek declaratory and injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs & the Class)

376. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

377. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

378. Defendant received a benefit from Plaintiffs in the form of Plaintiffs' Personal Information, including protected identifying information and protected health information covered by HIPAA and Michigan Law.

379. Defendant benefitted and continues to benefit from the use of Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at their expense.

380. Plaintiffs' Private Information has monetary value.

381. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Class Members and then disclosed to third parties without prior authorization and without any compensation.

382. Defendant consciously and surreptitiously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

383. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members.

384. Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

385. The benefits that Defendant derived from Plaintiffs and Class Members were not procured in a lawful manner. These benefits rightly belong to Plaintiffs and Class Members, who did not authorize or provide prior, informed consent to Defendant to disclose private and protected information provided to Defendant in order to seek and/or obtain substance use disorder services.

386. It would be inequitable under unjust enrichment principles in Michigan for Defendant to be permitted to retain any of the profit or other benefits wrongly and surreptitiously derived from the unfair, unlawful, and unconscionable methods, acts, and trade practices alleged in this Complaint.

387. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs & the Class)

388. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

389. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

390. When Plaintiffs and Class Members provided their user data and Private Information to Defendant in exchange for substance use and/or mental health services, they entered into an implied contract pursuant to which Defendant agreed to safeguard, protect, and not disclose their Private Information without prior, informed consent or written authorization.

391. Before Plaintiffs provided their user data and Private Information to Defendant, Defendant expressly promised to maintain the confidentiality of personally identifiable patient

data and communications. Defendant’s sign-up page promised that “All of the information you share is kept private and is protected by our HIPAA-compliant software.”⁷³

Sign up for Workit Health

Get started by answering a few questions to help us determine which program is right for you. All of the information you share is kept private and is protected by our HIPAA-compliant software.

Continue

392. After Workit users click on the “Continue” button to sign up with Defendant, the “Start your Workit profile” page once again assures users that “We take your privacy seriously. Your information is protected by our HIPAA compliant software.” Defendant’s statement prominently encourages users to provide personal and admittedly HIPAA-protected information to Defendant prior to signing up, with assurances that the private information they provide will be kept private.⁷⁴

⁷³ <https://app.workithealth.com/signup> (last visited June 27, 2023).

⁷⁴ https://app.workithealth.com/onboarding/zip_code (last visited June 27, 2023).

The screenshot shows a web form titled "Start your Workit profile". It contains five input fields: "First Name (Preferred) (Required)", "Date of Birth (Required)", "ZIP/Postal Code (Required)", and "How did you hear about us? (Required)" which is a dropdown menu. A green "Continue" button is positioned below the fields. At the bottom of the form, there is a privacy notice: "We take privacy seriously. Your information is protected by our HIPAA compliant software. [Learn more about our privacy practices.](#) Already scheduled an appointment over the phone? [Activate account](#) Already have an account? [Sign in](#)".

393. Users who click on the link entitled “Learn more about our privacy practices” are directed to the Workit Privacy Statement, which states that “Workit Health never exchanges data with a third party for any purpose other than improving the member experience, never sells data, and we only gather and request data from our members that will improve their quality of care within the program.”⁷⁵

⁷⁵ <https://www.workithealth.com/privacy-statement/> (last visited June 27, 2023).

394. Plaintiffs accepted Defendant's offers and provided their Private Information to Defendant in order to access substance use disorder services. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them, obligating Defendant to safeguard and protect their Private Information and not to disclose their Private Information without prior, informed consent and/or written authorization.

395. There was mutual assent and consideration for the implied agreement.

396. Plaintiffs performed their obligations under the implied agreement.

397. Defendant breached these implied contracts by failing to adequately safeguard and protect Plaintiffs' Private Information and by disclosing Plaintiffs' and Class Members' Private Information to third parties, i.e., Facebook and/or Google.

398. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their Private Information would be disclosed and/or inadequately safeguarded.

399. Plaintiffs and Class Members are entitled to nominal, compensatory, declaratory, and consequential damages as a result of Defendant's breaches of implied contract.

COUNT V
Negligence
(On Behalf of Plaintiffs & the Class)

400. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

401. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

402. Defendant, as a medical provider of substance use disorder services, has a common law duty to its patients to keep non-public medical information confidential.

403. Defendant also has a statutory duty to safeguard and protect records relating to the provision of substance use disorder services from unauthorized disclosure without the expressed, written consent of its patients. *See* MCL § 330.1262; MCL § 330.1263. Matters concerning a person’s medical treatment or condition are generally considered private and are protected by law, including HIPAA.

404. Michigan Law provides that “Records of the identity, diagnosis, prognosis, and treatment of an individual maintained in connection with the performance of a program, an approved service program, or an emergency medical service authorized or provided or assisted under this chapter are confidential[.]” MCL § 330.1261.

405. Michigan Law further provides that “Records of the diagnostic evaluation, psychiatric, psychological, social service care, and referral of an individual that are maintained in connection with the performance of an approved service program ... are confidential[.]” MCL § 330.1285.

406. Defendant is under a duty to safeguard and protect Private Information relating to Substance Use Disorder Services from unauthorized disclosure. *See* MCL § 330.1262; MCL § 330.1263.

407. Michigan Law does not allow for unauthorized disclosure of confidential information relating to Substance Use Disorder Services for Defendant’s private commercial purposes, including advertising or as a private revenue source, without a patient’s express, written consent.

408. As a medical provider of substance use disorder services, Defendant has a special relationship with Plaintiffs and Class Members, which separately and additionally gives rise to a common law legal duty.

409. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant through Defendant's Web Applications.

410. Plaintiffs' and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises on its website, and through its Privacy Statement, as alleged above.

411. By secretly, and without Plaintiffs' informed authorization, deploying surreptitious tracking technologies to disclose and transmit Plaintiffs' Private Information and the contents of their communications exchanged with Defendant to third parties, Defendant breached its duties to Plaintiffs and the Class.

412. Defendant's disclosures of Plaintiffs' and Class Members' Private Information were made without their knowledge, prior consent, or authorization.

413. The third-party recipients included, but were not limited to, Facebook and Google, which caused widespread dissemination of Plaintiffs' Private Information and caused them to be repeatedly subjected to unwanted and unauthorized microtargeted advertisements from Defendant and other service providers as a result.

414. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the health services provider and the patient.

415. As a direct and proximate cause of Defendant's unauthorized disclosures of patients' personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members suffered an actual, present injury to their privacy and property interests.

416. As a direct and proximate cause of Defendant's unauthorized disclosures of patients' personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members suffered injuries and damages resulting from Defendant's breach in that:

- a. Defendant's unlawful and unauthorized disclosure of Plaintiffs' Private Information caused Plaintiffs and Class Members to be repeatedly subjected to unwanted and unauthorized microtargeted advertisements from Defendant and other service providers who gained access to Plaintiffs' Private Information because of Defendant's disclosures;
- b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensating Plaintiffs for the data;
- e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- f. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information;

- g. Plaintiffs suffered emotional distress;
- h. Plaintiffs suffered loss of reputation; and
- i. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

417. Plaintiffs' on behalf of themselves and Class Members, seek nominal, compensatory, and punitive damages for Defendant's breaches of confidence.

COUNT VI
Unauthorized Disclosure of Privileged Communications
(On Behalf of Plaintiffs & the Class)

418. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

419. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

420. Defendant has a statutory duty to safeguard and protect records relating to the provision of substance use disorder services from unauthorized disclosure without the expressed, written consent of its patients. *See* MCL § 330.1262; MCL § 330.1263. Matters concerning a person's medical treatment or condition are generally considered private and are protected by law, including HIPAA.

421. Michigan Law provides that "Records of the identity, diagnosis, prognosis, and treatment of an individual maintained in connection with the performance of a program, an approved service program, or an emergency medical service authorized or provided or assisted under this chapter are confidential[.]" MCL § 330.1261.

422. Michigan Law further provides that "Records of the diagnostic evaluation, psychiatric, psychological, social service care, and referral of an individual that are maintained in

connection with the performance of an approved service program ... are confidential[.]” MCL § 330.1285.

423. Defendant is under a duty to safeguard and protect Private Information relating to Substance Use Disorder Services from unauthorized disclosure *See* MCL § 330.1262; MCL § 330.1263.

424. Information obtained by Defendant from Plaintiffs and Class Members are subject to the physician-patient privilege. *See* MCL § 600.2157.

425. Michigan recognizes a cause of action for the unauthorized disclosure of privileged communications. *Saur v. Probes*, 190 Mich. App. 636, 637, 476 N.W.2d 496, 498 (1991); *Alar v. Mercy Mem’l Hosp.*, 208 Mich. App. 518, 534, 529 N.W.2d 318, 325 (1995).

426. Michigan Law does not allow for disclosure of confidential information relating to Substance Use Disorder Services for Defendant’s private commercial purposes, including advertising or as a private revenue source, without a patient’s express, written consent.

427. Defendants’ disclosures of Plaintiffs’ and Class Members’ Private Information to third parties as alleged herein were made without their knowledge, consent, or authorization.

428. Plaintiffs and Class Members did not waive any privilege.

429. Defendant’s disclosure of Plaintiffs’ and Class Members’ Private Information was not justified by any supervening interest.

430. By secretly, and without Plaintiffs’ informed, consent or written authorization, deploying the Tracking Pixel and/or Google Analytics to acquire, disclose, and transmit Plaintiffs’ Private Information and the contents of their communications exchanged with Defendant to third parties, including Facebook and Google, Defendant violated Michigan Law, its ethical obligations,

and the physician-patient privilege, which requires that Plaintiffs' Private Information be maintained in confidence.

431. The third-party recipients included, but were not limited to, Facebook and Google, which caused widespread dissemination of Plaintiffs' Private Information and caused them to be repeatedly subjected to unwanted and unauthorized microtargeted advertisements from Defendant and other service providers as a result.

432. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the health services provider and the patient.

433. As a direct and proximate cause of Defendant's unauthorized disclosures of patients' personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members suffered damaged resulting from Defendant's breach in that:

- a. Defendant's unlawful and unauthorized disclosure of Plaintiffs' Private Information caused Plaintiffs and Class Members to be repeatedly subjected to unwanted and unauthorized microtargeted advertisements from Defendant and other service providers who gained access to Plaintiffs' Private Information because of Defendant's disclosures;
- b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;

- d. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensating Plaintiffs for the data;
- e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- f. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information;
- g. Plaintiffs suffered emotional distress;
- h. Plaintiffs suffered loss of reputation; and
- i. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

434. Plaintiffs, on behalf of themselves and Class Members, seek nominal, compensatory, and punitive damages for Defendant's breaches of confidence.

COUNT VII
Violations of the Michigan Consumer Protection Act (MCPA)
MCL § 445.901, et seq.
(On Behalf of Plaintiffs & the Class)

435. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

436. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

437. Defendant's conduct violates the MCPA, MCL 445.903 (Section 3), which provides that "[u]nfair, unconscionable, or deceptive methods, acts, or practices in the conduct of

trade or commerce are unlawful,” which includes “[e]ntering into a consumer transaction in which the consumer waives or purports to waive a right, benefit, or immunity provided by law, unless the waiver is clearly stated and the consumer has specifically consented to it.” MCL 445.903(t).

438. Plaintiffs and Class Members are “consumers” under the MCPA.

439. By providing information pursuant to the substance use disorder services offered through Defendant’s website and/or mobile app, and/or purchasing services through Defendant’s website or mobile app, Plaintiffs and Class Members entered into a consumer transaction with Defendant.

440. When entering into consumer transactions with Plaintiffs and Class Members, Defendant utilized the Tracking Pixel and/or Google Analytics to secretly acquire and disclose Plaintiffs’ and Class Members’ Private Information, including PII and PHI, to third parties, including Facebook and Google.

441. Defendant’s disclosure of Plaintiffs’ and Class Members’ Private Information, which included information that was required by law to be held in confidence pursuant to MCL § 330.1261, MCL § 330.1285, MCL § 600.2157, and HIPAA.

442. By unlawfully disclosing Plaintiffs’ confidential Private Information to third parties through the Tracking Pixel, Defendant intentionally, knowingly, and/or recklessly entered into a consumer transaction with Plaintiffs that caused Plaintiffs to waive privacy and confidentiality rights guaranteed by law.

443. Defendant failed to clearly state or disclose that by entering into a consumer transaction with Defendant that Plaintiffs and Class Members were waiving their confidentiality and privacy rights.

444. Rather, Defendant affirmatively and prominently promised Plaintiffs and the Class before they provided any information through Defendant’s website and/or mobile app that “[a]ll of the information you share is kept private and is protected by our HIPAA-compliant software.”⁷⁶

445. Defendant’s statement was knowingly false and misleading when made, given that Defendant knew that the tracking technologies it surreptitiously installed on its Website would transmit Plaintiffs’ confidential Private Information to third parties as part of the transaction, causing a waiver of Plaintiffs’ and Class Members’ legal rights.

446. Plaintiffs and Class Members did not consent to the waiver of their confidentiality rights or to the transmission of Plaintiffs’ Private Information to unknown third parties. Indeed, Defendant never provided Plaintiffs or Class Members with any opportunity to provide express, prior, written consent to waive their confidentiality rights in association with the consumer transaction.

447. As a direct and proximate result of Defendant’s unfair, unconscionable, and/or deceptive methods, acts, and/or practices, which are in violation of the MCPA, Plaintiffs and Class Members suffered losses and actual damages, in that:

- a. Defendant’s unlawful and unauthorized disclosure of Plaintiffs’ Private Information caused Plaintiffs and Class Members to be repeatedly subjected to unwanted and unauthorized microtargeted advertisements from Defendant and other service providers who gained access to Plaintiffs’ Private Information because of Defendant’s disclosures;

⁷⁶ <https://app.workithealth.com/signup> (last visited June 27, 2023).

- b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensating Plaintiffs for the data;
- e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- f. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and
- g. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

448. Plaintiffs, on behalf of themselves and Class Members, seek declaratory, equitable, and actual compensatory relief for Defendant's violations.

COUNT VIII
Violations of Electronic Communications Privacy Act
18 U.S.C. § 2511(1), et seq.
Unauthorized Interception, Use, and Disclosure
(On Behalf of Plaintiffs & the Class)

449. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

450. Plaintiffs bring this claim individually and on behalf of the members of the Class against Defendant.

451. The ECPA protects both sending and receipt of communications.

452. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

453. The transmissions of Plaintiffs' PII and PHI through Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

454. **Electronic Communications.** The transmission of Private Information, including PII and PHI, between Plaintiffs and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

455. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include [] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

456. **Interception.** The ECPA defines the interception as the “acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device” and “contents...include any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(4), (8).

457. **Electronic, Mechanical, or Other Device.** The ECPA defines “electronic, mechanical, or other device” as “any device...which can be used to intercept a[n]...electronic communication[.]” 18 U.S.C. § 2510(5). The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. Plaintiffs’ and Class Members’ browsers;
- b. Plaintiffs’ and Class Members’ computing devices;
- c. Defendant’s web servers;
- d. Defendant’s Website; and
- e. The Pixel code deployed by Defendant to effectuate the sending and acquisition of patient communications.

458. By secretly utilizing and embedding the Pixel and/or Google Analytics on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

459. Specifically, Defendant intercepted Plaintiffs’ and Class Members’ electronic communications via the Pixel and/or Google Analytics, which tracked, stored, and unlawfully disclosed Plaintiffs’ and Class Members’ Private Information, including PII and PHI, to Facebook and Google.

460. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs' and Class Members' regarding PII and PHI, treatment, medication, substance use programming, and scheduling.

461. By intentionally disclosing or endeavoring to disclose the electronic communications of the Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

462. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

463. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

464. Defendant was not acting under color of law to intercept Plaintiffs and the Class Member's wire or electronic communication.

465. Plaintiffs and Class Members did not authorize or provide prior, informed consent to Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via tracking code that Defendant intentionally installed and controlled on its Website.

466. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

467. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy and breach of confidentiality, among others.

468. The ECPA provides that a “party to the communication” may liable where a “communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C § 2511(2)(d).

469. Defendant is not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendant is a party, Defendant's simultaneous and surreptitious unknown duplication, forwarding, and interception of Plaintiffs' and Class members' Private Information does not qualify for the party exemption.

470. Defendant's acquisition of patient communications that were used and disclosed to Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and Michigan, including:

- a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;
- b. Violation of MCL § 330.1261;
- c. Violation of MCL § 600.2157 (physician-patient privilege) and
- d. MCL 445.903 (Michigan Consumer Protection Act).

471. Defendant sold or otherwise used patient communications for its own financial gain and enrichment with no benefit being conferred to Plaintiffs and the Class.

472. The penalty for violation is enhanced where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

473. Defendant’s conduct violated 42 U.S.C. § 1320d-6 in that it:

- a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and
- b. Disclosed individually identifiable health information to Facebook and Google without patients’ prior, informed consent or written authorization.

474. Defendant’s conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant’s use of the Facebook and Google source code was for Defendant’s commercial advantage to increase revenue from existing patients and gain new patients.

475. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs’ and Class Members’ communications about their PII and PHI on its Website, because it used its participation in these communications to improperly share Plaintiffs’ and Class Members’ PII and PHI with Facebook and Google, third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know was receiving their information, and that Plaintiffs and Class Members did not consent to receive this information.

476. As such, Defendant cannot viably claim any exception to ECPA liability.

477. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant’s invasion of privacy in that:

- a. Defendant intruded upon, acquired, intercepted, transmitted, shared, and used their individually identifiable patient health information (including information about their medical symptoms, conditions and concerns, medical appointments, healthcare providers and locations, medications and treatments and health insurance and medical bills) for impermissible and previously undisclosed commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;
- b. Plaintiffs suffered a loss of confidentiality in private and legally protected Private Information for undisclosed and impermissible purposes;
- c. Plaintiffs suffered a loss of privacy as a result of Defendant's unlawful acquisition of their private information for undisclosed and impermissible purposes;
- d. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' individually identifiable patient health information without providing any value or benefit to Plaintiffs or the Class Members;
- e. Defendant received substantial and quantifiable value from its use of Plaintiffs' and the Class Members' individually identifiable patient health information, such as understanding how people use its Website and determining

what ads people see on its Website, without providing any value or benefit to Plaintiffs or the Class Members;

- f. Plaintiffs lost value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;
- g. Plaintiffs were subjected to unwanted advertisements by Defendant and/or third parties as a result of Defendant's violation of their privacy and confidentiality;
- h. Diminished value of Plaintiffs' PII and PHI;
- i. General damages for invasions of privacy and confidentiality rights;
- j. Nominal damages; and
- k. Punitive damages.

478. As a result of Defendant's violation of the ECPA, Plaintiffs and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT IX
Violations of the California Invasion of Privacy Act (CIPA)
(On Behalf of Plaintiffs and the California Sub-Class)

479. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

480. Plaintiff Jane Doe 2 brings this claim individually and on behalf of the members of the California Sub-Class against Defendant.

481. Plaintiff Jane Doe 2 is a resident of California, and she provided Private Information through Defendant's Website and received services from Defendant while physically present in California.

482. Upon information and belief, hundreds of Class Members are residents of California and provided Private Information through Defendant's Website while physically present in California.

483. Defendant, through its Website, is engaged in the business of providing medical services to the Plaintiff Jane Doe 2 and the California Sub-Class.

484. Plaintiff Jane Doe 2 and the California Sub-Class used Defendant's Website to search for medical information, services and physicians, schedule appointments, and pay for medical services.

485. When Plaintiff Jane Doe 2 and the California Sub-Class used Defendant's Website, they were messaging, reporting, and/or communicating with Defendant.

486. Those messages, reports, and/or communications were transmitted or passed over a wire, line, or cable, and were sent from and/or received within California.

487. Defendant willfully disclosed the messages, reports, and/or communications with Facebook via the Facebook Pixel and/or with Google via Google Analytics, which were under Defendant's discretion and control at all times relevant hereto.

488. By doing so, Defendant willfully aided and permitted Facebook and/or Google, third parties, to read and learn of the messages, reports, and/or communications between the Plaintiff/California Sub-Class and Defendant.

489. Plaintiff Jane Doe 2 and the California Sub-Class did not consent to Defendant aiding or permitting Facebook, Google, and/or other third parties to read or learn about the messages, reports, or communications between them and Defendant.

490. Defendant is liable to Plaintiff Jane Doe 2 and the California Sub-Class for statutory damages of \$5,000 for each time it disclosed a message, report, or communication to Facebook and/or Google without consent or authorization.

491. At all times relevant hereto, in violation of Penal Code § 631(a), Defendant aided, agreed with, employed and/or conspired with Facebook and/or Google to engage in, permit, or cause to be done the unauthorized reading and/or use of messages and communications from Plaintiff Jane Doe 2 and members of the California Sub-Class while the same were in transit or passing over a wire, line, or cable, for which Plaintiff seeks and is entitled to recover, inter alia, penalties under Penal Code § 637(a) on behalf of Plaintiff Jane Doe 2 and the California Sub-Class for each violation of Penal Code § 631(a) committed by Defendant against Plaintiff Jane Doe 2 and/or members of the California Sub-Class.

COUNT X
Violations of the California Confidentiality of Medical Information Act (CMIA)
(On Behalf of Plaintiffs & the California Sub-Class)

492. Plaintiffs repeat, re-allege, and incorporate by reference each and every allegation contained in the Complaint as if fully set forth herein.

493. Plaintiff Jane Doe 2 brings this claim individually and on behalf of the members of the California Sub-Class against Defendant.

494. Plaintiff Jane Doe 2 is a resident of California, and she provided Private Information through Defendant's Website, and Defendant offered and provided Plaintiff Jane Doe 2 services while she was physically present in California.

495. Upon information and belief, hundreds of Class Members are residents of California and provided Private Information through Defendant's Website while physically present in California.

496. Defendant is a provider of healthcare pursuant to California Civil Code § 56.06(b).

497. Plaintiff Jane Doe 2 and Members of the California Sub-Class are patients, enrollees, and subscribers of Defendant.

498. Plaintiff and the California Sub-Class used Defendant's Website to, inter alia, search for medical treatments, services and physicians, schedule appointments, and pay for medical services.

499. Plaintiff disclosed this medical information about Plaintiff Jane Doe 2 and the California Sub-Class with Facebook via Facebook Pixel and with Google via Google Analytics, through tracking tools under Defendant's sole discretion and control.

500. Defendant's sharing, sale, and/or use of the Plaintiff's and the California Sub-Class' medical information was done intentionally, willfully, and/or negligently.

501. The disclosures of Plaintiff Jane Doe 2 and the California Sub-Class' medical information was not for any purpose necessary to providing healthcare services.

502. Plaintiff Jane Doe 2 and the California Sub-Class were not aware Defendant was sharing, selling, or using their medical information.

503. Plaintiff Jane Doe 2 and the California Sub-Class did not authorize the sharing, sale, or use of their medical information.

504. Defendant is liable to the Plaintiff Jane Doe 2 and the California Sub-Class for statutory damages of \$1,000 for each time it shared, sold, or used their medical information without authorization for purposes not necessary to providing healthcare services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully pray for judgment in their favor against Defendant Workit Health (MI), PLLC as follows:

- A. Certification of the Classes by order pursuant to Fed.R.Civ.P. 23;
- B. Designation of Plaintiffs as representatives of the proposed Class and designation of Plaintiffs' counsel as Class counsel;
- C. Judgment in favor of Plaintiffs and Class Members as against the Defendant;
- D. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- E. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI disclosed to third parties;
- F. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

- G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- H. For declaratory and/or injunctive relief;
- I. For an award of punitive damages, as allowable by law;
- J. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees, including pre- and post-judgment interest;
- K. Pre- and post-judgment interest on any amounts awarded; and
- L. Such other and further relief as this court may deem just and proper.

Date: July 14, 2023

Respectfully submitted,

/s/ Nicholas A. Coulson

Nicholas A. Coulson

Steven D. Liddle

Matthew Z. Robb

LIDDLE SHEETS COULSON P.C.

975 East Jefferson Avenue

Detroit, MI 48207-3101

T: (313) 392-0015

F: (313) 392-0025

E: sliddle@lscounsel.com

E: ncoulson@lscounsel.com

E: mrobb@lscounsel.com

/s/ David S. Almeida

David S. Almeida*

Elena A. Belov*

ALMEIDA LAW GROUP LLC

849 W. Webster Avenue

Chicago, Illinois 60614

T: (312) 576-3024

E: david@almeidawgroup.com

E: elena@almeidawgroup.com

Attorneys for Plaintiffs & Putative Classes
** Pro Hac Vice applications forthcoming*

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: July 14, 2023

Respectfully submitted,

/s/ Nicholas A. Coulson

Nicholas A. Coulson

Matthew Z. Robb

LITTLE SHEETS COULSON P.C.

975 East Jefferson Avenue

Detroit, MI 48207-3101

T: (313) 392-0015

F: (313) 392-0025

E: ncoulson@lscounsel.com

E: mrobb@lscounsel.com

David S. Almeida*

Elena A. Belov*

*Pro Hac Vice applications to be submitted

ALMEIDA LAW GROUP LLC

849 W. Webster Avenue

Chicago, Illinois 60614

T: (312) 576-3024

E: david@almeidawgroup.com

E: elena@almeidawgroup.com

Attorneys for Plaintiffs & Putative Classes

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [\\$578K Workit Health Settlement Resolves Class Action Lawsuit Over Alleged Data Sharing With Facebook, Google](#)
