

1 Alan M. Mansfield (SBN: 125998)
2 WHATLEY KALLAS LLP
3 1 Sansome Street, 35th Floor
4 PMB #131
5 San Francisco, CA 94104 /
6 16870 West Bernardo Drive, Ste 400
7 San Diego, CA 92127
8 Phone: (619) 308-5034
9 Fax: (888) 341-5048
10 Email: amansfield@whatleykallas.com

William J. Doyle (SBN: 188069)
Chris W. Cantrell (SBN 290874)
DOYLE APC
550 West B Street
4th Floor
San Diego, CA 92101
Phone: (619) 736-0000
Fax: (619) 736-1111
Email: bill@doyleapc.com
chris@doyleapc.com

6 April M. Strauss (SBN 163327)
7 APRIL M. STRAUSS, A PC
8 2500 Mountain View Drive, Bldg 3
9 Mountain View, CA 94040
10 Phone: (650) 281-7081
11 Email: astrauss@sfaclp.com

12 *Attorneys for Plaintiff*

11 UNITED STATES DISTRICT COURT
12 NORTHERN DISTRICT OF CALIFORNIA
13 SAN JOSE DIVISION

14 JANE DOE, individually and on behalf of all
15 others similarly situated,

16 Plaintiff,

17 vs.

18 BETTERHELP, INC. AND DOES 1-10,
19 inclusive,

20 Defendants.
21

Case No.: **5:23-cv-01096**

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

1 Plaintiff Jane Doe, on behalf of herself and all others similarly situated, asserts the following
2 against Defendants BetterHelp, Inc. and DOES 1-10 inclusive, based upon personal knowledge
3 where so identified and otherwise on information and belief and the investigation of counsel, which
4 included consultation with experts in the field of data privacy, as to all other matters.

5 **SUMMARY OF ALLEGATIONS**

6 1. BetterHelp Inc. (“BetterHelp”) is a telehealth company based in California that
7 operates through the website <https://BetterHelp.com/>. It claims on its website to be “the world’s
8 largest therapy platform” and is described as a “mental health platform that provides online mental
9 health services directly to consumers. The online counseling and therapy services are provided
10 through web-based interaction as well as phone and text communication.” It is reported that
11 BetterHelp has served over 1 million patients nationwide over the last several years.

12 2. BetterHelp has offered mental health services under several different business names,
13 including MyTherapist; Teen Counseling; Faithful Counseling; Pride Counseling; iCounseling;
14 Regain; and Terapeuta. BetterHelp is a membership-based service that charges members from \$60-
15 \$90 per week.

16 3. BetterHelp encourages patients to use its website to research their medical symptoms
17 and health issues, identify therapists who can treat their specific conditions, and take other actions
18 related to their health care. When doing this, patients convey highly private information, including
19 medical information, through BetterHelp’s website.

20 4. When a user enters health information through BetterHelp’s website and patient
21 portals, medical information—including, in some instances, specifically what the user is seeking
22 treatment for—is sent to BetterHelp, whose function is to work with patients with particular issues
23 such as anxiety and depression. Companies can obtain a treasure trove of personal medical
24 information about the user simply by virtue of the user accessing this particular site.

25 5. Both BetterHelp and the websites it operated, as well as third-party websites and
26 organizations such as those linked to surreptitiously by BetterHelp such as Facebook, Snapchat,
27 Criteo, and Pinterest, benefit from the ability to analyze a user’s experience and activity on its
28 website to assess the website’s functionality and traffic. These third-party websites also gain

1 information about their customers that can be used to target/retarget them with advertisements and
2 to measure the results of advertisement efforts.

3 6. According to the United States Federal Trade Commission, BetterHelp (under its
4 name and all of its other business names) used consumers' email addresses and the fact they had
5 been in therapy to instruct Facebook to identify similar consumers and target them with
6 advertisements for BetterHelp's counseling service. The FTC further alleges that BetterHelp misled
7 consumers about keeping their mental health information private and using various unauthorized
8 methods shared data with companies such as Facebook, Snapchat, Criteo, and Pinterest to advertise
9 its services.

10 7. Under various arrangements set forth below, BetterHelp thus transmitted to third
11 parties portions of patients' private communications for the primary, if not the sole purpose of
12 sharing such information with marketing entities. BetterHelp's goal in that transmittal of private
13 communications was not to provide any benefit to its patients but instead to (1) increase its
14 marketshare through the identification of new potential patients and the recapture/retention of prior
15 patients, and (2) to cultivate and maintain relationships with various social media sites.

16 8. Unbeknownst to users and without their consent, third parties such as Facebook and
17 thereby its operating company Meta Platforms Inc. ("Meta") gained the ability to surreptitiously
18 gather user interaction ranging from what a user clicks on to the personal information entered on a
19 BetterHelp website by use of invisible online trackers placed on BetterHealth website pages. These
20 only trackers then send users unsolicited advertisements based on that tracking information. This
21 data, which can include health conditions, diagnoses, procedures, treatment status, the treating
22 physician, medications, and PII (hereinafter "User Data"), is viewed, obtained, and used by
23 companies such as Facebook in connection with targeted advertising.

24 9. Plaintiff Jane Doe had her User Data, including sensitive medical information,
25 harvested through BetterHelp's website without her consent when he entered information on the
26 BetterHelp patient portal, and continued to have her privacy violated when her User Data was used
27 for profit after BetterHelp and third-parties like Meta, sold her sensitive and confidential User Data
28 to pharmaceutical and other companies that used this User Data to send Plaintiff targeted advertising

1 related to medical conditions he was attempting to obtain treatment for through BetterHelp’s
2 website.

3 10. As a result of this illegal information gathering, Plaintiff received advertisements that
4 were specifically tailored to her User Data, including sensitive medical information, that he entered
5 on BetterHelp patient portals, thereby providing other third parties with access to persons most likely
6 to be interested in their products or services

7 11. BetterHelp knows that the User Data it collects and transfers to third parties includes
8 highly sensitive medical information but, in either conscious or reckless disregard for patient
9 privacy, continued to collect, use, and profit from this information, and were sharing and permitting
10 companies like Meta, Snapchat, Criteo, and Pinterest to use Plaintiff’s and the Class members’ User
11 Data, including sensitive medical information.

12 12. Defendant’s actions constitute an extreme invasion of Plaintiff and Class members’
13 right to privacy and violate several statutory and common law doctrines, including the California
14 Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 631, *et seq.*; the California Constitution Article
15 I, Section I; California’s Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*;
16 California’s Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.*; California’s Online
17 Privacy Protection Act, California Business and Professions Code §§ 22575-22579 (“CalOPPA”);
18 the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.* (“FTC Act”), the HIPAA Privacy Rule
19 and Security Rule, 45 C.F.R. Parts 160 and 164; and common law doctrines such as breach of
20 implied contracts, breach of fiduciary duty and breach of confidence.

21 13. Plaintiff Jane Doe and the Class Members seek remedies for violations of the
22 aforementioned statutes and common law doctrines.

23 **PARTIES**

24 **A. Plaintiff**

25 14. On personal knowledge, Plaintiff Jane Doe (“Plaintiff Doe” or “Jane Doe”) is a
26 resident of Grand Haven, Michigan.

27 15. On personal knowledge, Plaintiff Doe is a Facebook user and has had a Facebook
28 account since at least 2007.

1 16. On personal knowledge, Plaintiff Doe is a user of the BetterHelp website and web
2 portal since October 2021.

3 17. On personal knowledge, to make appointments, Plaintiff was required to utilize the
4 online portals associated with and created by BetterHelp.

5 18. On personal knowledge, simply to sign up to use BetterHelp and use these patient
6 portals entailed Plaintiff entering her User Data, including sensitive medical information, sexuality
7 questions, gender, age, religious preferences, relationship status, therapy experiences, reasons for
8 seeking therapy, financial, physical and mental health questions, and other personal information
9 requested by BetterHelp during the initial questionnaire process.

10 19. On personal knowledge, after entering this information on the BetterHelp website,
11 Plaintiff began to receive targeted advertisements on her Facebook page and other locations that
12 appear to have been related to the information she provided BetterHelp.

13 **B. Defendants**

14 20. Defendant BetterHelp, Inc., also doing business as Compile, Inc.; MyTherapist; Teen
15 Counseling; Faithful Counseling; Pride Counseling; iCounseling; ReGain; and Terapeuta, is a
16 Delaware corporation with its principal office or place of business located at 990 Villa St., Mountain
17 View, CA 94041. BetterHelp operates in and from California through the website
18 <https://BetterHelp.com/>. The company services millions of patients nationwide. According to the
19 FTC: “Since BetterHelp was founded, more than two million people have signed up, entrusting the
20 company with their personal information, much of it related to the status of their health – and their
21 mental health.” On January 9, 2023 it was announced that BetterHelp raked in over \$1 billion in
22 revenue, which was a \$300 million increase from 2021, with over 1 million people using its platform
23 in 2022.

24 21. Through the wrongful conduct at issue herein, since at some point in 2017 BetterHelp
25 has allowed companies like Meta, Snapchat, Criteo, and Pinterest to surreptitiously collect user data
26 such as provided by Plaintiff and others and associate it with Plaintiff’s and other Class Members’
27 Facebook and other accounts for use in targeting them with advertisements. This private information
28 was also used to target other individuals for advertising and to increase the profits of BetterHelp and

1 third party social media companies.

2 22. The true names, roles, and capacities in terms of their involvement in the wrongdoing
3 at issue, whether individual, corporate, associate, or otherwise, of Defendants named as Does 1
4 through 10, inclusive, are currently unknown to Plaintiff and, therefore, are named as Defendants
5 under fictitious names. Plaintiff will identify these Defendants' true identities and their involvement
6 in the wrongdoing at issue if and when they become known.

7 **JURISDICTION AND VENUE**

8 23. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C
9 § 1332(d), because the amount in controversy for the Class exceeds \$5,000,000 exclusive of interest
10 and costs, there are more than 100 putative class members defined below, and minimal diversity
11 exists because a significant portion of putative class members are citizens of a state different from
12 the citizenship of at least one Defendant.

13 24. This Court has general personal jurisdiction over BetterHelp because it maintains its
14 principal place of business in California. Additionally, BetterHelp is subject to specific personal
15 jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiff's
16 and others' claims occurred in or arose out of actions taken this State.

17 25. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), (c), and (d) because
18 BetterHelp is based in this District, transacts business in this District and a substantial portion of the
19 events giving rise to the claims occurred in this District.

20 **DIVISIONAL ASSIGNMENT**

21 26. The proper divisional assignment for this matter is the San Jose Division. Defendant
22 BetterHelp, Inc., is, and was at all times material hereto, headquartered in Mountain View located
23 in the County of Santa Clara, California. A substantial part of the events and conduct giving rise to
24 the claims herein occurred in or arose out of BetterHelp's headquarters in Santa Clara, California.
25 Pursuant to L.R. 3.2(e), all civil actions that arise in the county of Santa Clara shall be assigned to
26 the San Jose Division of the Northern District.

FACTUAL ALLEGATIONS

A. BACKGROUND OF CALIFORNIA LAWS PROTECTING PRIVACY

27. In California, the protection of personal privacy is of paramount importance. Article 1, section 1 of the California Constitution guarantees consumers their right to privacy. In addition, as recognized by the California State Legislature, the use of computer information technology has greatly magnified the potential risk to individual privacy that occurs from the maintenance of personal information by entities such as Defendant, necessitating that the maintenance of personal information is subject to strict limits governed by numerous California statutes.

28. Under California law, medical information is considered to be among the most sensitive private personal information available. “Medical Information” is defined by California’s Confidential Medical Information Act, Cal. Civ. Code sections 56, et seq. (“CMIA”) as:

any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment.

29. “Individually identifiable” means that the Medical Information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or Social Security Number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.

30. “Personal and Medical Information”, for purposes of this Complaint, refers to the above definition and encompasses both Personal Health Information (“PHI”), and Personally Identifiable Information (“PII”), including information associated with individual’s health maintained within BetterHelp’s computer systems.

31. Since PHI and PII encompass personal and revealing information, it is highly valued. PHI and PII hves been found to command up to \$1,000 per individual record.

32. Under the CMIA and other laws as set forth herein, Plaintiff and Class members have a recognized right to confidentiality in their Personal and Medical Information and can reasonably expect that their Personal and Medical Information would be protected by Defendant from

1 unauthorized access. When Plaintiff and Class members provided their Personal and Medical
2 Information to BetterHelp for the purpose of enrollment, maintaining an account with BetterHelp,
3 seeking coverage for medical treatment and otherwise availing themselves of health care services
4 through BetterHelp, they did so with the reasonable understanding and assurance that their Personal
5 and Medical Information would be kept confidential and secure.

6 33. The Historical and Statutory Notes for the short title of the CMIA, § 56, support these
7 reasonable expectations:

8 The Legislature hereby finds and declares that persons receiving health care
9 services have a right to expect that the confidentiality of individually identifiable
10 Medical Information derived by health service providers be reasonably preserved.
11 It is the intention of the Legislature in enacting this act, to provide for the
12 confidentiality of individually identifiable Medical Information, while permitting
13 certain reasonable and limited uses of that information.

14 Stats. 1981, ch. 782, § 1, p. 3040.

15 34. Consistent with that statutory purpose, the CMIA provides that “a provider of health
16 care, health care service plan, or contractor shall not disclose Medical Information regarding a
17 patient of the provider of health care or an enrollee or subscriber of a health care service plan without
18 first obtaining an authorization [. . .].” Cal. Civ. Code § 56.10(a). Defendant’s actions disclosed
19 and/or permitted the disclosure of the Personal and Medical Information at issue here to
20 unauthorized third parties.

21 35. Additionally, Cal. Civ. Code § 56.101(a) states, in relevant part, that every provider
22 of health care provider or, health care service plan or contractor that creates, maintains, preserves,
23 or stores Personal and Medical Information shall do so in a manner that preserves its confidentiality.
24 Defendant’s actions establish that they did not maintain the Personal and Medical Information at
25 issue in a manner that preserved its confidentiality. BetterHelp’s failure to create, maintain, preserve,
26 and store Personal and Medical Information in a manner that preserved the confidentiality of the
27 information contained therein resulted in the illegal access, authorization, exfiltration, disclosure,
28 and negligent release of well over 200,000 personal unique records, which necessarily included
Personal and Medical Information, to known parties such as Meta.

1 **B. BETTERHELP ILLEGALLY TRANSMITTED CONFIDENTIAL USER DATA TO**
2 **THIRD PARTIES FOR UNSOLICITED ADVERTISING AND TO ENRICH**
3 **ITSELF AND OTHER THIRD PARTY SOCIAL MEDIA COMPANIES**

4 36. On March 2, 2023, the United States Federal Trade Commission announced it had
5 entered into a proposed settlement with Mountain View, California based BetterHelp, Inc. banning
6 it from sharing website user data for advertising purposes as well as a \$7.8 million fine that may be
7 used to provide partial consumer refunds to people who signed up for and paid for BetterHelp’s
8 services between August 1, 2017, and December 31, 2020 (although it appears such tracking has
9 continued without adequate or any disclosure of the true facts).

10 37. On BetterHelp’s website, patients are asked to answer a series of questions covering
11 their mental health conditions. Although BetterHelp’s website claims that information is kept private
12 and safeguarded, this information is reportedly sent to advertising platforms, along with the
13 information needed to identify users. This data is extremely personal, and it can be used to target
14 advertisements for services that, as the United States Senate has stated in an investigation of other
15 similar health care provider companies, may be “potentially harmful physically, psychologically, or
16 emotionally.”

17 38. Critically, on its website BetterHelp represents: “We have built state-of-the-art
18 technology, operations, and infrastructure with the goal of protecting your privacy and safeguarding
19 the information you provide.” Despite those promises, the FTC alleges BetterHelp used a wide
20 variety of tactics to share the health information of over 7 million consumers. For example, in 2017,
21 BetterHelp allegedly uploaded the email addresses of all of its current and former clients to Facebook
22 – nearly 2 million in total – to target them with ads to refer their Facebook friends to BetterHelp for
23 mental health services.

24 39. According to a Complaint filed by the FTC against BetterHelp: “In 2017,
25 [BetterHelp] delegated most decision-making authority over its use of Facebook’s advertising
26 services to a Junior Marketing Analyst who was a recent college graduate, had never worked in
27 marketing, and had no experience and little training in safeguarding consumers’ health information
28 when using that information for advertising. In doing so, [BetterHelp] t gave the Junior Marketing
Analyst carte blanche to decide which Visitors’ and Users’ health information to upload to Facebook

1 and how to use that information. This same individual, who now holds the title “Senior Marketing
2 Analyst,” continues to oversee [BetterHelp]’s use of Facebook’s advertising tools.”

3 40. The FTC alleges BetterHelp “compiled lists of Visitors’ and Users’ email addresses,
4 which it then uploaded to Facebook to match these individuals to their Facebook user accounts in
5 order to target them and others like them with advertisements. Between 2017 and 2018, [BetterHelp]
6 uploaded lists of over 7 million Visitors’ and Users’ email addresses to Facebook. Facebook matched
7 over 4 million of these Visitors and Users with their Facebook user IDs, linking their use of the
8 Service for mental health treatment with their Facebook accounts. Several examples are listed below:

9 (a) January 2017 – October 2018: [BetterHelp] uploaded over 170,000 Visitors’ and
10 Users’ email addresses to Facebook, re-targeting these individuals and targeting
11 potential new Users with advertisements for the Service.

12 (b) January 2018 – October 2018: [BetterHelp] uploaded over 15,000 Users’ email
13 addresses to Facebook to find and target new potential Users with advertisements for
14 the Service.

15 (c) October 2017: [BetterHelp] uploaded the email addresses of all their current and
16 former Users—nearly 2 million in total—to Facebook, targeting them all with
17 advertisements to refer their Facebook friends to the Service.

18 41. The FTC Complaint further alleges “Second, from 2013 to December 2020,
19 [BetterHelp] shared Visitors’ and Users’ email addresses, IP addresses, and records known as
20 “Events” with Facebook. These Events automatically tracked certain actions of each Visitor and
21 User on the Multi-Sites, such as when they answered certain questions on the Intake Questionnaire
22 in a certain way or when a Visitor enrolled in the Service to become a User. [BetterHelp] recorded
23 and automatically disclosed these Events to Facebook through web beacons [BetterHelp] had placed
24 on each of the Multi-Sites. [BetterHelp] disclosed Visitors’ and Users’ IP addresses, email addresses,
25 and/or other persistent identifiers to Facebook alongside the Events so that Facebook could match
26 the Events information with the Visitors’ and Users’ Facebook accounts for advertising. Several
27 examples are listed below:

28 (a) January 2018: [BetterHelp] disclosed to Facebook that over 70,000 Visitors had

1 signed up for accounts (but had not become paying Users)—through an Event
2 denoting as much—in order to re-target them with advertisements for the Service.

3 (b) November 2018 – March 2020: [BetterHelp] disclosed to Facebook over 1.5 million
4 Visitors’ and Users’ previous therapy—gathered through their affirmative responses
5 to the Intake Questionnaire question “Have you been in counseling or therapy
6 before?”—to re-target the Visitors with advertisements and optimize [BetterHelp]’s
7 advertisements.

8 (c) October 2018 – November 2020: [BetterHelp] used and shared over 3.5 million
9 Visitors’ and Users’ “good” or “fair” financial status—gathered through the Intake
10 Questionnaire—with Facebook to optimize [BetterHelp]’s advertisements and to find
11 potential new Users and target them with advertisements.

12 (d) January – December 2020: [BetterHelp] shared with Facebook the fact that over
13 180,000 Visitors had become paying Users—through an Event denoting they had
14 entered credit card information after completing the Intake Questionnaire—to
15 optimize [BetterHelp]’s advertisements and to find potential new Users and target
16 them with advertisements. [BetterHelp] labeled the Intake Questionnaire responses
17 concerning prior therapy and financial status with anonymous Event titles before
18 giving them to Facebook; however, in July 2018, the previously mentioned
19 inexperienced and insufficiently trained Junior Marketing Analyst whom
20 [BetterHelp] had put in charge of Facebook advertising revealed certain Events’ true
21 meaning to Facebook via the Facebook employee that serviced [BetterHelp]’s
22 advertising account. For example, though an affirmative response to the question
23 “Have you been in counseling or therapy before?” was coded as “AddToWishlist,”
24 the analyst revealed to Facebook that this event meant that the “user completes
25 questionnaire marking they have been in therapy before,” thereby disclosing millions
26 of Visitors’ and Users’ prior therapy to Facebook.

27 42. The FTC Complaint goes on to describe Health information that BetterHelp shared
28 with other third parties: “In January 2019, [BetterHelp] disclosed to Snapchat the IP addresses and

1 email addresses of approximately 5.6 million Visitors to re-target them with advertisements for the
2 Service. From July 2018 to January 2019, [BetterHelp] disclosed the email addresses of over 70,000
3 Visitors—including Pride Counseling and Faithful Counseling Visitors—to Criteo in order to re-
4 target them with advertisements. And, from August 2019 to September 2020, [BetterHelp] disclosed
5 Visitors' email addresses to Pinterest for advertising. Additional use of health information for
6 advertising: From November 2017 to October 2020, [BetterHelp] used information concerning
7 approximately 600,000 Pride Counseling Visitors' or Users' mental health statuses and their
8 connection with the Visitors' and Users' LGBTQ identities to optimize future advertisements for
9 the Service on Facebook. [BetterHelp] gathered this information through the Intake Questionnaire
10 whenever a Pride Counseling Visitor or User revealed that the Visitor's or User's "LGBTQ identity
11 is contributing to your mental health concerns." [BetterHelp] used Facebook to identify
12 characteristics and interests common among these Visitors and Users and then to target future
13 advertisements for the Service on Facebook to individuals with similar characteristics and interests.

14 43. As a result of these intentional, reckless or negligent acts and practices, Plaintiff and
15 other Class members who signed up for and paid for BetterHelp's services since at least August 1,
16 2017, and through a date to be determined, had their personal information sold to third party
17 advertisers such as Facebook, Snapchat, Criteo, and Pinterest without their informed authorization
18 or consent.

19 44. The federal government recently issued a warning to companies such as BetterHelp
20 that sharing of such data may violate federal privacy laws. For example in a statement entitled USE
21 OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND
22 BUSINESS ASSOCIATES (the "Bulletin"), recently issued by the Department of Health and
23 Human Services Office for Civil Rights ("OCR"), it stated that while healthcare organizations
24 regulated under HIPAA may use third-party tracking tools in a limited way, such as to perform
25 analysis on data key to its operations, they are not permitted to use these tools in a way that may
26 expose patients' protected health information to these vendors. The Bulletin explains:

27 Regulated entities [those to which HIPAA applies] are not permitted to use tracking
28 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

1 example, disclosures of PHI to tracking technology vendors for marketing purposes,
2 without individuals' HIPAA-compliant authorizations, would constitute
impermissible disclosures.

3 45. The Bulletin also identified the types of harm that disclosure may cause to the patient:

4 "An impermissible disclosure of an individual's PHI not only violates the Privacy
5 Rule but also may result in a wide range of additional harms to the individual or
6 others. For example, an impermissible disclosure of PHI may result in identity theft,
7 financial loss, discrimination, stigma, mental anguish, or other serious negative
8 consequences to the reputation, health, or physical safety of the individual or to
9 others identified in the individual's PHI. Such disclosures can reveal incredibly
10 sensitive information about an individual, including diagnoses, frequency of visits to
11 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."

12 46. Plaintiff and Class members have no idea that Defendant is collecting and utilizing
13 their User Data, including sensitive medical information, when they engage with websites such as
14 those operated by BetterHelp because the software that provides such surreptitious access is
15 incorporated in the background.

16 47. For instance, when Plaintiff logged into Defendant's patient portal, there was no
17 indication or disclosure that it would collect and share personal sensitive medical information.

18 48. Plaintiff, and all Class members, could not consent to Defendant's conduct when they
19 were unaware their sensitive medical information would be collected and used in the first place.

20 49. BetterHelp was aware that sharing such data would result in the disclosure and use
21 of Plaintiff's and Class members' personal information, including sensitive medical information. As
22 it never disclosed the presence of this tracking and surveillance process, Defendant did not obtain
23 users' consent to collect, use, and store Plaintiff's and Class members' sensitive medical
24 information.

25 **C. PLAINTIFF AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION**
26 **OF PRIVACY IN THEIR USER DATA, ESPECIALLY WITH RESPECT TO**
27 **SENSITIVE MEDICAL INFORMATION**

28 50. Plaintiff and Class members have a reasonable expectation of privacy in their User
Data, including personal information and sensitive medical information. Defendant surreptitiously

1 collected and used Plaintiff and Class members' User Data, including, highly sensitive medical
2 information, in violation of Plaintiff's and Class members' reasonable expectations of privacy.

3 51. According to the FTC: "In the hierarchy of confidential data, health information ranks
4 right up there. And in the hierarchy of health information, details about a person's mental health
5 may be among the most confidential. But according to the FTC, that's not how online counseling
6 service BetterHelp viewed it. The FTC says the company repeatedly pushed people to take an Intake
7 Questionnaire and hand over sensitive health information through unavoidable prompts."

8 52. Privacy polls and studies show that almost all Americans consider one of the most
9 important privacy rights to be the need for an individual's affirmative consent before a company
10 collects and shares its customers' data, and thus the actions of companies such as BetterHelp to be
11 material to them. For example, a recent study by Consumer Reports shows that 92% of Americans
12 believe that internet companies and websites should be required to obtain consent before selling or
13 sharing consumers' data, and the same percentage believe internet companies and websites should
14 be required to provide consumers with a complete list of the data that has been collected about them.¹
15 Moreover, according to a study by Pew Research Center, approximately 79% of Americans are
16 concerned about how data is collected about them by companies.²

17 53. The concern about sharing medical information is compounded by the reality that
18 advertisers view this type of information as particularly high value. Indeed, having access to the data
19 women share with their healthcare providers allows advertisers to obtain data on children before
20 they are even born. As one article put it: "the datafication of family life can begin from the moment
21 in which a parent thinks about having a baby."³ The article continues "Children today are the very
22 first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the

23
24 ¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*,
CONSUMER REPORTS (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

25
26 ² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER, (Nov. 15, 2019),
27 <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

28 ³ Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, THE MIT PRESS READER, <https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/>.

1 social and political consequences of this historical transformation. What is particularly worrying
2 about this process of datafication of children is that companies like . . . Facebook . . . are harnessing
3 and collecting multiple typologies of children’s data and have the potential to store a plurality of
4 data traces under unique ID profiles.”⁴

5 54. Defendant is required by the CMIA and other California laws identified herein, and
6 various other laws and regulations to protect Plaintiff’s and Class members’ Personal and Medical
7 Information and to handle notification of any breach in accordance with applicable breach
8 notification statutes. These duties are established in numerous California statutes, including Cal.
9 Civ. Code §§ 56.10(a), 56.101, 1798.21, 1798.29, Cal. Bus. and Prof. Code §§ 17200 et seq.,
10 Cal. Bus. and Prof. Code §§ 22575-2257, Cal. Penal Code § 630-632 et seq., as well as Article I, § 1
11 of the California Constitution. Failing to do so results in acts of negligence *per se* by Defendant.

12 55. The California Invasion of Privacy Act (CIPA) which makes it unlawful for
13 businesses to engage in electronic “wire tapping” without consent or helping other entities, like
14 Facebook, intercept electronic communications without consumer consent. The CIPA may entitle
15 consumers to \$5,000 or three times their damages, whichever is greater.

16 56. In addition, as Defendant is an entity covered by HIPAA and various contracts
17 require it do so, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R.
18 Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health
19 Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected
20 Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national
21 security standards and duties for Defendant’s protection of Personal and Medical Information
22 maintained by them in electronic form. HIPAA limits the permissible uses of health information and
23 prohibits the disclosure of this information without explicit authorization. *See* 45 C.F.R. § 164.502.
24 HIPAA also requires that covered entities implement appropriate safeguards to protect this
25 information. *See* 45 C.F.R. § 164.530(c)(1).

26 57. HIPAA requires Defendant to “comply with the applicable standards,
27 implementation specifications, and requirements” of HIPAA “with respect to electronic protected

28 ⁴ *Id.*

1 health information.” 45 C.F.R. § 164.302.

2 58. “Electronic protected health information” is defined as “individually identifiable
3 health information ... that is (i) transmitted by electronic media; maintained in electronic media.” 45
4 C.F.R. § 160.103.

5 59. HIPAA’s Security Rule requires Defendant to: (a) ensure the confidentiality,
6 integrity, and availability of all electronic protected health information the covered entity or business
7 associate creates, receives, maintains, or transmits; (b) protect against any reasonably anticipated
8 threats or hazards to the security or integrity of such information; (c) protect against any reasonably
9 anticipated uses or disclosures of such information that are not permitted; and (d) ensure compliance
10 by its workforce.

11 60. HIPAA also requires Defendant to “review and modify the security measures
12 implemented . . . as needed to continue provision of reasonable and appropriate protection of
13 electronic protected health information.” 45 C.F.R. § 164.306(c), and also to “[i]mplement technical
14 policies and procedures for electronic information systems that maintain electronic protected health
15 information to allow access only to those persons or software programs that have been granted access
16 rights.” 45 C.F.R. § 164.312(a)(1).

17 61. Defendant failed to comply with safeguards mandated by HIPAA regulations,
18 including, but not limited to, the following:

- 19 (a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendant
20 creates, receives, maintains, and transmits, in violation of 45 C.F.R. section
21 164.306(a)(1);
- 22 (b) Failing to implement technical policies and procedures for electronic information
23 systems that maintain electronic PHI to allow access only to those persons or software
24 programs that have been granted access rights such as by the use of multi factor
25 authentication, in violation of 45 C.F.R. section 164.312(a)(1);
- 26 (c) Failing to implement policies and procedures to prevent, detect, contain, and correct
27 security violations, in violation of 45 C.F.R. section 164.308(a)(1);
- 28 (d) Failing to identify and respond to suspected or known security incidents and mitigate,

1 to the extent practicable, harmful effects of security incidents that are known to the
2 covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

3 (e) Failing to protect against any reasonably-anticipated threats or hazards to the security
4 or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

5 (f) Failing to protect against any reasonably anticipated uses or disclosures of electronic
6 PHI that are not permitted under the privacy rules regarding individually identifiable
7 health information, in violation of 45 C.F.R. section 164.306(a)(3);

8 (g) Failing to ensure compliance with HIPAA security standard rules by its workforce
9 by providing for adequate comprehensive training rather than simply using training
10 software to test staff by imitating phishing emails, in violation of 45 C.F.R. section
11 164.306(a)(4);

12 (h) Impermissibly and improperly using and disclosing PHI that is and remains
13 accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, et seq.;

14 (i) Failing to effectively train all members of its workforce (including independent
15 contractors) on the policies and procedures with respect to PHI as necessary and
16 appropriate for the members of its workforce to carry out their functions and to
17 maintain security of PHI beyond simply using training software to test staff by
18 imitating phishing emails, in violation of 45 C.F.R. sections 164.530(b) and
19 164.308(a)(5); and

20 (j) Failing to design, implement, and enforce policies and procedures establishing
21 physical and administrative safeguards to reasonably safeguard PHI in compliance
22 with violation of 45 C.F.R. section 164.530(c).

23 62. Defendant also violated the duties applicable to it under the Federal Trade
24 Commission Act, 15 U.S.C. § 45 *et seq.* (“FTC Act”), from engaging in “unfair or deceptive acts or
25 practices in or affecting commerce.” The FTC pursuant to that Act has concluded that a company’s
26 failure to maintain reasonable and appropriate data security for consumers’ sensitive personal
27 information is an “unfair practice” in violation of the FTC Act.

28 63. As established by these laws, Defendant owed a duty to Plaintiff and Class members

1 to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting
2 the Personal and Medical Information in its possession from being misused by unauthorized persons
3 such as the companies identified herein. This also included a duty to Plaintiff and Class members to
4 design, maintain, and test its computer systems to ensure that the Personal and Medical Information
5 in its possession was adequately secured and protected; to create and implement reasonable data
6 security practices and procedures to protect the Personal and Medical Information in its possession;
7 and to disclose if its computer systems and data security practices were inadequate to safeguard
8 individuals' Personal and Medical Information.

9 64. By taking affirmative acts inconsistent with these obligations, Defendant disclosed
10 and permitted the disclosure of Personal and Medical Information to unauthorized third parties.
11 Through such actions or inactions, BetterHelp failed to preserve the confidentiality of Personal and
12 Medical Information it was duty-bound to protect.

13 65. As a direct and proximate result of Defendant's breaches of its fiduciary duties,
14 Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i)
15 actual identity compromise; (ii) the loss of the opportunity how their Personal and Medical
16 Information is used; (iii) the compromise and publication of their Personal and Medical Information
17 to unauthorized third parties; (iv) lost opportunity costs associated with effort expended and the loss
18 of productivity addressing and attempting to mitigate the actual present and future consequences of
19 the unlawful sharing of their Personal and Medical Information, including but not limited to time
20 and effort spent researching how to prevent, detect, contest, and recover from fraud and identity theft
21 and implementing measures to do so; and (v) present and future costs in terms of time, effort, and
22 money that will be expended to prevent, detect, contest, and repair the impact of the Personal and
23 Medical Information compromised by Defendant's actions.

24 **D. THE VALUE OF PERSONAL AND MEDICAL INFORMATION SHOWS THAT**
25 **PLAINTIFFS AND OTHERS LOST VALUABLE MONEY OR PROPERTY**

26 66. It is well known that Personal and Medical Information is a valuable commodity such
27 that Plaintiff and Class members would lose money or property if their data was permitted to be
28 improperly accessed.

1 67. According to Experian, one of the three major credit bureaus, medical records can be
2 worth up to \$1,000 per person, depending upon completeness. PII and PHI can be sold at a price
3 ranging from approximately \$20 to \$300.

4 68. Time Magazine in an article entitled “HOW YOUR MEDICAL DATA FUELS A
5 HIDDEN MULTI-BILLION DOLLAR INDUSTRY” referenced the “growth of the big health data
6 bazaar,” in which patients’ health information is sold. It reported that: “[T]he secondary market in
7 information unrelated to a patient’s direct treatment poses growing risks, privacy experts say. That’s
8 because clues in anonymized patient dossiers make it possible for outsiders to determine your
9 identity, especially as computing power advances in the future.”

10 **TOLLING, CONCEALMENT, AND ESTOPPEL**

11 69. The applicable statutes of limitation have been tolled as a result of Defendant’s
12 knowing and active concealment and denial of the facts alleged herein.

13 70. Defendant had exclusive knowledge of these material facts yet failed to disclose that
14 by interacting with the BetterHelp that Plaintiff and Class members’ sensitive medical information
15 would be collected, used, and stored by unauthorized third parties.

16 71. Plaintiff and Class Members could not with due diligence have discovered the full
17 scope of Defendant’s conduct, including because there were no disclosures or other indication that
18 they were sharing such data.

19 72. The earliest Plaintiff and Class members, acting with due diligence, could have
20 reasonably discovered this conduct would have been on March 2, 2023, when the FTC announced
21 its settlement with BetterHelp.

22 73. All applicable statutes of limitation also have been tolled by operation of the
23 discovery rule. Under the circumstances, Defendant was under a duty to disclose the nature and
24 significance of their data collection practices but did not do so. Defendant is therefore estopped from
25 relying on any potentially applicable statute of limitations.

26
27
28

CLASS ACTION ALLEGATIONS

1
2 74. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23
3 individually and on behalf of the following Class:

4 All natural persons in the United States whose User Data was collected through
5 BetterHelp websites through third party on-line tracking codes since August 1,
6 2017.

7 75. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action
8 and any members of their immediate families; (2) the Defendant, Defendant’s subsidiaries, affiliates,
9 parents, successors, predecessors, and any entity in which the Defendant or its parents have a
10 controlling interest and its current or former employees, officers, and directors; and (3) Plaintiff’s
11 counsel and Defendant’s counsel.

12 76. The exact number of members of the Class is unknown and unavailable to Plaintiff
13 at this time, but individual joinder in this case is impracticable. The Class likely consists of over 1
14 million individuals, and the members can be identified through BetterHelp’s records.

15 77. The Classes’ claims present common questions of law and fact, and those questions
16 predominate over any questions that may affect individual Class members. Common questions for
17 the Classes include, but are not limited to, the following:

- 18 • Whether Defendant implemented and maintained reasonable security practices and
19 procedures appropriate to protect Plaintiff’s and Class members’ Personal and
20 Medical Information from unauthorized access, or disclosure;
- 21 • Whether Defendant and its employees, agents, officers, or directors negligently or
22 unlawfully disclosed or permitted the unauthorized disclosure of Plaintiff’s and Class
23 members’ Personal and Medical Information to unauthorized persons;
- 24 • Whether Defendant negligently created, maintained, preserved, stored, abandoned,
25 or disposed of Plaintiff’s and Class members’ Personal and Medical Information, and
26 failed to protect and preserve the integrity of the Personal and Medical Information
27 found on BetterHelp’s systems;
- 28 • Whether Defendant’s actions or inactions were a proximate result of the negligent or

1 reckless release of confidential information or records concerning Plaintiff and the
2 Class;

- 3 • Whether Defendant adequately, promptly, timely, and accurately informed Plaintiff
4 and the Class members that their Personal and Medical Information had been
5 compromised and whether Defendant violated the law by failing to promptly and
6 fully notify Plaintiff and the Class members of this material fact;
- 7 • Whether Defendant engaged in “unfair” business practices by failing to safeguard the
8 Personal and Medical Information of Plaintiff and the Class, and whether
9 Defendant’s violations of the state and federal laws cited herein constitute “unlawful”
10 business practices in violation of California Business and Professions Code § 17200,
11 et seq.;
- 12 • Whether Defendant violated the California Medical Information Act, the California
13 Invasion of Privacy Act, and the other laws cited herein; and
- 14 • Whether Plaintiff and the Class are entitled to damages, equitable and injunctive
15 relief to redress the imminent and currently ongoing harm faced as a result of the this
16 unauthorized disclosure and Defendant’s failure to provide full and adequate notice
17 thereof, and the scope of such relief.

18 78. Plaintiff’s claims are typical of the claims of the other members of the Class. The
19 claims of Plaintiff and the members of the Class arise from the same conduct by Defendant and are
20 based on the same legal theories.

21 79. Plaintiff has and will continue to fairly and adequately represent and protect the
22 interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation
23 and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is
24 materially antagonistic to the interests of the Class, and Defendant has no defenses unique to any
25 Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of
26 the members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel
27 have any interest materially adverse to the interests of the other members of the Class.

28 80. This class action is appropriate for certification because class proceedings are

1 superior to other available methods for the fair and efficient adjudication of this controversy and
2 joinder of all members of the Class is impracticable. This proposed class action presents fewer
3 management difficulties than individual litigation, and provides the benefits of single adjudication,
4 economies of scale, and comprehensive supervision by a single court. Class treatment will create
5 economies of time, effort, and expense and promote uniform decision-making.

6 81. Plaintiff reserves the right to revise the class allegations and definitions based on facts
7 learned and legal developments following additional investigation, discovery, or otherwise.

8 **CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS**

9 82. California substantive laws apply to every member of the Class. California's
10 substantive laws may be constitutionally applied to the claims of Plaintiff and the Classes under the
11 Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S.
12 Constitution. California has significant contact, or significant aggregation of contacts, to the claims
13 asserted by Plaintiff and Class members, thereby creating state interests to ensure that the choice of
14 California state law is not arbitrary or unfair.

15 83. BetterHelp's principal place of business is located in and it conducts substantial
16 business in California such that California has an interest in regulating BetterHelp's conduct under
17 its laws. BetterHelp's decision to reside in California and avail itself of California's laws, renders
18 the application of California law to the claims herein constitutionally permissible. The conduct at
19 issue also originated in and emanated from California as that is where the decisions to include the
20 tracking processes at issue were made and likely effectuated, and where the illegal data transfers
21 took place. BetterHelp communicated with third parties such as meta and the other third parties
22 identified herein while this data was in transit or was being sent from or received within California
23 through servers maintained by either BetterHelp or third parties such as Meta and the other third
24 parties identified herein in this State.

25 84. The application of California laws to the Class is also appropriate under California's
26 choice of law rules because California has significant contacts to the claims of Plaintiff and the
27 proposed Class, and California has a greater interest in applying its laws here than any other
28 interested state.

FIRST CLAIM FOR RELIEF

Violation of the Confidentiality of Medical Information Act

(Cal. Civ. Code § 56 *et seq.*)

1
2
3
4 85. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein
5 to the extent relevant to this Claim for Relief and the relief available thereunder.

6 86. California Civil Code § 56.06(d) specifically provides that (d) “[a]ny business that
7 offers a mental health digital service to a consumer for the purpose of allowing the individual to
8 manage the individual’s information, or for the diagnosis, treatment, or management of a medical
9 condition of the individual, shall be deemed to be a provider of health care subject to the
10 requirements of this part.” Thus, Defendant is, by statutory definition under the CMIA a “provider
11 of health care” subject to the Act.

12 87. Additionally, Defendant is a “health care service plan”, “provider of health care”
13 and/or a “recipient” of Personal and Medical Information as defined by Cal. Civ. Code § 56.05(d)
14 and (m), § 56.06(a) and (b) and/or Section 56.13 and are therefore subject to the requirements of the
15 CMIA.

16 88. Defendant must not disclose or permit the disclosure of Personal and Medical
17 Information regarding a patient of the provider of health care or an enrollee or subscriber of a health
18 care service plan without first obtaining authorization, subject to certain exceptions found in Cal.
19 Civ. Code §§ 56.10(b) & (c) that do not apply here. Cal. Civ. Code § 56.10(a). By its affirmative
20 acts and inactions set forth above, Defendant disclosed or permitted the disclosure of Personal and
21 Medical Information to unauthorized third parties, in violation of this Section.

22 89. Defendant is required under the CMIA to ensure that it maintains, preserves, and
23 stores Personal and Medical Information in a manner that preserves the confidentiality of the
24 information contained therein. Cal. Civ. Code §§ 56.101(a) & 56.36(b).

25 90. Defendant is required to create, maintain, preserve, store, abandon, destroy, or
26 dispose of Personal and Medical Information in a non-negligent manner. Cal. Civ. Code § 56.101(a).

27 91. Defendant’s electronic health record systems or electronic medical record systems
28 are required to protect and preserve the integrity of electronic Personal and Medical Information.

1 Cal. Civ. Code § 56.101(b)(1)(A). The term “electronic health record” or “electronic medical record”
2 means an electronic record of health-related information on an individual that is created, gathered,
3 managed, and consulted by authorized health care clinicians and staff. Cal. Civ. Code § 56.101(c)
4 as defined by 42 U.S.C. § 17921(5).

5 92. Plaintiff and members of the Class are “Patients” as defined by Cal. Civ. Code section
6 56.05(j).

7 93. A significant portion of the information at issue in this action is “Medical
8 Information” as that term is defined by § 56.05(i) of the CMIA.

9 94. As described above, the actions or inactions of Defendants failed to preserve the
10 confidentiality of Personal and Medical Information, including but not limited to Plaintiff’s and
11 Class members’ full names, dates of birth, addresses, medical and participant information that, either
12 alone or in combination with other publicly available information, reveals their identities.

13 95. The tracking codes used by BetterHelp and surreptitiously embedded in its website
14 made possible the linking of a BetterHelp website user and their identity. The information
15 exchanged, including the contents of searches and the act and substance of ordering medications
16 and other services provided on that website, and even the mere use of that website in light of the
17 services offered, reveals information about patients’ “physical condition or history.”

18 96. As a proximate result of the wrongful conduct detailed herein, Defendant has
19 released, disclosed, and/or negligently allowed third parties that are known to Defendants,
20 including Meta and other third parties as identified herein to access and view Plaintiff’s and Class
21 members’ medical information without first obtaining their written authorization as required by the
22 provisions of Civil Code § 56, et seq.

23 97. As a further result of the Defendant’s actions, the confidential nature of the Plaintiff’s
24 and Class members’ medical information was breached due to Defendant’s negligence or affirmative
25 decisions.

26 98. The Personal and Medical Information was accessed, removed, and viewed by
27 unauthorized third parties including Meta, Snapchat, Criteo, Pinterest and other unauthorized parties
28 by virtue of surreptitious code embedded in BetterHelp’s website.

1 99. In violation of the CMIA, Defendant disclosed or permitted the disclosure of Personal
2 and Medical Information regarding Plaintiff and Class members without authorization to a third
3 party. This disclosure did not qualify for any of the exemptions set forth in Cal. Civ. Code §§
4 56.10(b) or (c), which provide limited bases for allowing unauthorized disclosures. This disclosure
5 of Personal and Medical Information to unauthorized individuals resulted from the affirmative
6 actions and inactions of Defendant and its employees.

7 100. In violation of the CMIA, Defendant created, maintained, preserved, stored,
8 abandoned, or disposed of Personal and Medical Information of Plaintiff and Class members in a
9 manner that did not preserve the confidentiality of the information contained therein.

10 101. In violation of the CMIA, Defendant negligently created, maintained, preserved,
11 stored, abandoned, or disposed of Personal and Medical Information of Plaintiff and Class members.

12 102. In violation of the CMIA, Defendant's electronic health record systems or electronic
13 medical record systems did not protect and preserve the integrity of Plaintiff's and Class members'
14 Personal and Medical Information.

15 103. In violation of the CMIA, Defendant negligently released confidential or medical
16 information or records concerning Plaintiff and Class members. Defendant also violated § 56.101(a)
17 of the CMIA, which prohibits the negligent sharing and release of Plaintiff's and Class members'
18 Personal and Medical Information.

19 104. In violation of the CMIA, as a recipient of medical information pursuant to an
20 authorization it disclosed and/or permitted the disclosure of that medical information without
21 obtaining a new authorization that meets the requirements of Section 56.11, or as specifically
22 required or permitted by law.

23 105. As a direct and proximate result of Defendant's breaches of its duties, Plaintiff and
24 Class members have suffered and will suffer injury, including, but not limited to: (i) actual identity
25 compromise; (ii) the loss of the opportunity how their Personal and Medical Information is used;
26 (iii) the compromise and publication of their Personal and Medical Information to unauthorized third
27 parties; (iv) time and expenses associated with the prevention, detection, and recovery from identity
28 theft, tax fraud, or other unauthorized use of their Personal and Medical Information; (v) lost

1 opportunity costs associated with effort expended and the loss of productivity addressing and
2 attempting to mitigate the actual present and future consequences of the unlawful sharing of their
3 Personal and Medical Information, including but not limited to time and effort spent researching
4 how to prevent, detect, contest, and recover from fraud and identity theft and implementing measures
5 to do so; and the continued risk to their Personal and Medical Information, which remain in
6 Defendant's possession, custody or control and is subject to further unauthorized disclosures so long
7 as Defendant fails to undertake appropriate and adequate measures to protect the Personal and
8 Medical Information of current and former patients and their beneficiaries and dependents; and (vi)
9 present and future costs in terms of time, effort, and money that will be expended to prevent, detect,
10 contest, and repair the impact of the Personal and Medical Information compromised by Defendant's
11 actions.

12 106. Plaintiff and Class members are therefore entitled to injunctive relief and reasonable
13 attorneys' fees and costs.

14 107. Plaintiff seeks actual damages for Class members, statutory damages of \$1,000 per
15 Class member and punitive damages of \$3,000 per Class member. In order to recover under the
16 CMIA, Civil Code Section 56.36 expressly states that it is not necessary that the plaintiff suffered
17 or was threatened with actual damages.

18 **SECOND CLAIM FOR RELIEF**

19 **Violation of the California Invasion of Privacy Act**

20 **(Cal. Penal Code §§ 630, 631, *et seq.* ("CIPA"))**

21 108. Plaintiff incorporates the foregoing allegations as if fully set forth herein to the extent
22 relevant to this Claim for Relief and the relief available thereunder.

23 109. California's Invasion of Privacy Act, California Penal Code 631(a) provides a
24 remedy against, inter alia: Any person who ... intentionally taps, or makes any unauthorized
25 connection, whether physically, electrically, ..., or otherwise, with any telegraph or telephone wire,
26 line, cable, or instrument ... or who willfully and without the consent of all parties to the
27 communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents
28 or meaning of any message, report, or communication while the same is in transit or passing over

1 any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses,
2 or attempts to use, in any manner, or for any purpose, or to communicate in any way, any
3 information so obtained, or who aids, agrees with, employs, or conspires with any person or persons
4 to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this
5 section, Defendant BetterHelp is a person for the purposes of this law.

6 110. Defendant “intentionally tap[ped] ... or ma[de] [an] unauthorized connection”
7 with respect to Class members’ communications by placing third party tracking code on its website,
8 without “the consent of all parties” including Plaintiff, and thereby violated the CIPA.

9 111. Defendant also “aid[ed], agree[d] with, employ[d], or conspire[d] with” various third
10 parties including providing marketing services by allowing such entities to “tap” communications
11 on its website without “the consent of all parties” including Plaintiff, and thereby violated CIPA.

12 112. Defendant facilitated the interception and simultaneous transmission to Meta,
13 Snapchat, Criteo, Pinterest and other third party advertisers of Plaintiff’s and other Class members’
14 PII and PHI while the information was “in transit” without their informed authorization or consent

15 113. The information communicated between patients and BetterHelp was transmitted to
16 or from the State of California. The information was wiretapped “while the same is in transit or
17 passing over any wire, line, or cable, or is being sent from, or received at any place within this state.”

18 114. Redirection of data as a result of tracker coding before that data reaches its originally
19 intended recipient (here, BetterHelp) does not constitute a separate communication for the purposes
20 of exclusion from CIPA coverage.

21 115. BetterHelp enabled non-parties to the communications to “read” the communications
22 for the purposes of the statute. For example, Meta, Snapchat, Criteo, Pinterest and other third parties
23 could see which individuals searched for specific issues, what conditions they researched, and when
24 and where they made appointments.

25 116. BetterHelp facilitated this communication “without authorization” of Class members
26 because it did not give Class members any hint that the transmission was happening.

27 117. Class members did not request that Defendant and third parties target them with
28 advertising that might be related to their health conditions.

1 118. Cal. Penal Code § 637.2(a) provides that any person who has been injured by a
2 violation of this chapter [including Penal Code §§ 630 and 631] may bring an action against the
3 person who committed the violation for the greater of the following amounts:

4 (1) Five thousand dollars (\$5,000) per violation.

5 (2) Three times the amount of actual damages, if any, sustained by the plaintiff.

6 119. Cal. Penal Code § 637.2(b) provides that “[a]ny person may . . . bring an action to
7 enjoin and restrain any violation of this chapter, and may in the same action seek damages as
8 provided by subdivision (a).”

9 120. Cal. Penal Code § 637.2(c) provides, “It is not a necessary prerequisite to an
10 action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.”

11 121. Defendant is therefore liable to Plaintiff and the Class for, at a minimum, statutory
12 damages of \$5,000 per violation as well as actual damages, and Plaintiff and Class members are also
13 entitled to injunctive relief.

14 **THIRD CLAIM FOR RELIEF**

15 **Violation of the California Invasion of Privacy Act**

16 **(Cal. Penal Code § 632, et seq.)**

17 122. Plaintiff incorporates the foregoing allegations as if fully set forth herein to the extent
18 relevant to this Claim for Relief and the relief available thereunder.

19 123. Cal. Penal Code § 632 provides, in relevant part, that it is unlawful to “intentionally
20 and without the consent of all parties to a confidential communication,” “use[] [a] recording device
21 to . . . record the confidential communication.” As used in the statute “‘confidential communication’
22 means any communication carried on in circumstances as may reasonably indicate that any party to
23 the communication desires it to be confined to the parties thereto.”

24 124. The written transmission of information about Plaintiff’s and Class members’
25 searches and clicks on BetterHelp’s website as described above is a recording of those
26 communications.

27 125. Defendant did not have Plaintiff’s or other Class members’ consent to record their
28 communications.

1 126. Cal. Penal Code § 637.2(a) provides that any person who has been injured by a
2 violation of this chapter [including Penal Code § 632] may bring an action against the person who
3 committed the violation for the greater of the following amounts:

4 (1) Five thousand dollars (\$5,000) per violation.

5 (2) Three times the amount of actual damages, if any, sustained by the plaintiff.

6 127. Cal. Penal Code § 637.2(b) provides that “[a]ny person may . . . bring an action to
7 enjoin and restrain any violation of this chapter, and may in the same action seek damages as
8 provided by subdivision (a).”

9 128. Cal. Penal Code § 637.2(c) provides, “It is not a necessary prerequisite to an action
10 pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.”

11 129. Defendant is therefore liable to Plaintiff and the Class for, at a minimum, statutory
12 damages of \$5,000 per violation and actual damages. Plaintiff and Class members are also entitled
13 to injunctive relief.

14 **FOURTH CLAIM FOR RELIEF**

15 **Invasion of Privacy**

16 **(California Constitution, Article I, Section 1)**

17 130. Plaintiff incorporate the foregoing allegations by reference as if fully set forth herein
18 to the extent relevant to this Claim for Relief and the relief available thereunder.

19 131. The California Constitution provides: “All people are by nature free and independent
20 and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring,
21 possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy.”
22 Cal. Const., Art. I., § 1.

23 132. Plaintiff and Class members had a legitimate expectation of privacy in their Personal
24 and Medical Information, and were entitled to the protection of this information against disclosure
25 to unauthorized third parties.

26 133. Defendant owed a duty to Plaintiff and Class members to keep their Personal and
27 Medical Information confidential.

28 134. Defendant failed to protect and released to unauthorized third parties the Personal

1 and Medical Information of Plaintiff and Class members.

2 135. Defendant allowed unauthorized third parties such as Meta, Snapchat, Criteo,
3 Pinterest and others access to and examination of the Personal and Medical Information of Plaintiff
4 and Class members by way of Defendant's affirmative actions and negligent failures to protect this
5 information.

6 136. The unauthorized release to, custody of, and examination by unauthorized third
7 parties of the Personal and Medical Information of Plaintiff and Class members is highly offensive
8 to a reasonable person.

9 137. The intrusion at issue was into a place or thing, which was private and is entitled to
10 be private. Plaintiff and Class members disclosed their Personal and Medical Information to
11 Defendant as part of Plaintiff's and Class members' relationships with Defendant, but privately and
12 with the intention that the Personal and Medical Information would be kept confidential and would
13 be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their
14 belief that such information would be kept private and would not be disclosed without their
15 authorization or affirmative consent.

16 138. The sharing of data that resulted from the actions and inactions of Defendant
17 constitutes an intentional interference with Plaintiff's and Class members' interest in solitude or
18 seclusion, either as to their persons or as to their private affairs or concerns and those of their
19 families, of a kind that would be highly offensive to a reasonable person.

20 139. Defendant either knew or reasonably should have known that its inadequate and
21 insufficient information security practices would cause injury and harm to Plaintiff and Class
22 members.

23 140. As a proximate result of the above acts and omissions of Defendant, the Personal and
24 Medical Information of Plaintiff and Class members was disclosed to third parties without
25 authorization, causing Plaintiff and Class members to suffer injuries and damages.

26 141. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful
27 conduct will continue to cause irreparable injury to Plaintiff and the Class, entitling them to seek
28 injunctive relief. Plaintiff also seek damages to the fullest extent permitted by law.

1 142. This action, if successful, will enforce an important right affecting the public interest
2 and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of
3 persons and the general public. Private enforcement is necessary and places a disproportionate
4 financial burden on Plaintiff in relation to Plaintiff's stake in the matter. Because this case is brought
5 for the purposes of enforcing important rights affecting the public interest, Plaintiff also seeks the
6 recovery of attorneys' fees and costs in prosecuting this action against Defendant under Cal. Code
7 Civ. Proc. § 1021.5 and other applicable law.

8 **FIFTH CLAIM FOR RELIEF**

9 **Negligence and Negligence Per Se**

10 143. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein
11 to the extent relevant to this Claim for Relief and the relief available thereunder.

12 144. Defendant knowingly collected, came into possession of, and maintained Plaintiff's
13 and Class members' Personal and Medical Information, and had a duty to exercise reasonable care
14 in safeguarding, securing, and protecting such information from being compromised, misused, and
15 disclosed to unauthorized parties.

16 145. As a provider of health care under California law, Defendant had a special
17 relationship with Plaintiff and Class members who entrusted Defendant with adequately protecting
18 their Personal and Medical Information.

19 146. Defendant knew that the Personal and Medical Information was private and
20 confidential and should be protected as private and confidential, and thus, Defendant owed a duty
21 of care not to subject Plaintiff and Class members to an unreasonable risk of unauthorized disclosure.

22 147. Defendant knew, or should have known, of the risks inherent in collecting and storing
23 Personal and Medical Information, and the importance of not permitting unauthorized access to such
24 sensitive information.

25 148. Defendant's failure to take proper security measures to protect Plaintiff and Class
26 member's Personal and Medical Information created conditions conducive to a foreseeable,
27 intentional criminal act, namely the unauthorized access and exfiltration of Personal and Medical
28 Information by unauthorized third parties. As described above, Plaintiff and Class members are part

1 of a foreseeable, discernable group that was at high risk of having their Personal and Medical
2 Information compromised, and otherwise wrongly disclosed if not adequately protected by
3 Defendant.

4 149. Defendant had a duty under common law to have procedures in place to detect and
5 prevent the loss or unauthorized dissemination of Plaintiff's and Class members' Personal and
6 Medical Information.

7 150. Defendant had a duty to employ reasonable security measures, systems, processes,
8 and otherwise protect the Personal and Medical Information of Plaintiff and Class members pursuant
9 to the state and federal laws set forth above, resulting in Defendant's liability under principles of
10 negligence and negligence per se.

11 151. Defendant owed a duty to timely and adequately inform Plaintiff and Class members,
12 in the event of a data breach, that their Personal and Medical Information had been improperly
13 disclosed to unauthorized third parties.

14 152. Defendant systematically failed to provide adequate security for data in its possession
15 or over which they had supervision and control.

16 153. Defendant, through its actions and omissions, unlawfully breached duties to Plaintiff
17 and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's
18 and Class members' Personal and Medical Information within Defendant's possession, supervision,
19 and control.

20 154. Defendant, through its actions and omissions, unlawfully breached duties owed to
21 Plaintiff and Class members by failing to have appropriate procedures in place to prevent
22 dissemination of Plaintiff's and Class members' Personal and Medical Information.

23 155. Defendant, through its actions and omissions, unlawfully breached duties to timely
24 and fully disclose to Plaintiff and Class members that the Personal and Medical Information within
25 Defendant's possession, supervision, and control was compromised, the nature of the compromise,
26 and precisely the type of information compromised by being accessed by unauthorized third parties.

27 156. Defendant's breach of duties owed to Plaintiff and Class members proximately
28 caused Plaintiff's and Class members' Personal and Medical Information to be compromised.

1 157. As a result of Defendant’s ongoing failure to adequately notify Plaintiff and Class
2 members regarding what type of Personal and Medical Information has been compromised, Plaintiff
3 and Class members are unable to take the necessary precautions to mitigate damages.

4 158. Pursuant to the laws set forth herein, including Cal. Civ. Code s§ 56.10(a), 56.101,
5 1798.21, 1798.29 and Article I, § 1 of the California Constitution. Defendant acts also violated
6 federal statutes and regulations, including the FTC Act, HIPAA, the HIPAA Privacy Rule and
7 Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of
8 Individually Identifiable Health Information”), and Security Rule (“Security Standards for the
9 Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts
10 A and C and the other sections identified above, Defendant was required by law to maintain adequate
11 and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff’s
12 and Class members’ Personal and Medical Information.

13 159. Plaintiff and Class members are within the class of persons that these statutes and
14 rules were designed to protect.

15 160. It was reasonably foreseeable, indeed it was intended, that the failure to reasonably
16 protect and secure Plaintiff’s and Class members’ Personal and Medical Information in compliance
17 with applicable laws would result in unauthorized third-parties gaining access to Plaintiff’s and Class
18 members’ Personal and Medical Information resulting in Defendant’s liability under principles of
19 negligence per se.

20 161. Plaintiff’s and Class members’ Personal and Medical Information constitutes
21 personal property that was taken and misused as a proximate result of Defendant’s negligence,
22 resulting in harm, injury and damages to Plaintiff and Class members. As a proximate result of
23 Defendant’s negligence and breach of duties as set forth above, Defendant’s breaches of duty caused
24 Plaintiff and Class members to suffer receiving unwanted advertisements that reveal seeking
25 treatment for specific medical conditions, fear, anxiety and worry about the status of their Personal
26 and Medical Information, diminution in the value of their personal data for which there is a tangible
27 value and loss of control over their Personal and Medical Information, all of which can constitute
28 actionable actual damages.

1 162. In failing to secure Plaintiff's and Class members' Personal and Medical Information,
2 Defendant is guilty of oppression, fraud, or malice. Defendant acted or failed to act with a reckless,
3 willful, or conscious disregard of Plaintiff's and Class members' rights. Plaintiff, in addition to
4 seeking actual damages, also seeks punitive damages on behalf of themselves and the Class.

5 163. Defendant's conduct in violation of applicable laws directly and proximately caused
6 the unauthorized access and disclosure of Plaintiff's and Class members' Personal and Medical
7 Information and Plaintiff and Class members have suffered and will continue to suffer damages as
8 a result of Defendant's conduct. Plaintiff and Class members seek actual, compensatory, and
9 punitive damages, and all other relief they may be entitled to as a proximate result of Defendant's
10 negligence and negligence *per se*.

11 **SIXTH CLAIM FOR RELIEF**

12 **Breach of Confidence**

13 164. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein
14 to the extent relevant to this Claim for Relief and the relief available thereunder.

15 165. At all times during Plaintiff's and Class members' interactions with Defendant,
16 Defendant was required to be aware of the confidential and sensitive nature of Plaintiff's and the
17 Class members' Personal and Medical Information that Plaintiff and Class members provided to
18 Defendant.

19 166. As alleged herein, Defendant's relationship with Plaintiff and Class members was
20 governed by the reasonable expectations that Plaintiff's and the Class members' Personal and
21 Medical Information would be collected, stored, and protected in confidence, and would not be
22 disclosed to unauthorized third parties.

23 167. Plaintiff and Class members provided their Personal and Medical Information with
24 the explicit and implicit understandings that it would be protected and that such Personal and
25 Medical Information would not be disseminated to any unauthorized third parties, and that the
26 persons who had access to such data would take precautions to protect that Personal and Medical
27 Information from unauthorized disclosure. These explicit or implicit understandings and
28 relationships are evidenced by the numerous contractual provisions set forth above that imposed on

1 Defendant a contractual obligation to ensure such Personal and Medical Information was protected
2 from unauthorized access.

3 168. Defendant voluntarily received in confidence Plaintiff's and Class members'
4 Personal and Medical Information with the understanding that such information would not be
5 disclosed or disseminated to the public or any unauthorized third parties.

6 169. As a proximate result of Defendant's failure to prevent and protect this unauthorized
7 disclosure, Plaintiff's and Class members' Personal and Medical Information was disclosed and
8 misappropriated to unauthorized third parties beyond Plaintiff's and the Class members' confidence,
9 and without their express permission.

10 170. As a direct and proximate result of Defendant's breaches of its duties, Plaintiff and
11 Class members have suffered and will suffer injury, including, but not limited to: (i) actual identity
12 compromise; (ii) the loss of the opportunity how their Personal and Medical Information is used;
13 (iii) the compromise and publication of their Personal and Medical Information to unauthorized third
14 parties; (iv) time and expenses associated with the prevention, detection, and recovery from identity
15 theft, tax fraud, or other unauthorized use of their Personal and Medical Information; (v) lost
16 opportunity costs associated with effort expended and the loss of productivity addressing and
17 attempting to mitigate the actual present and future consequences of the unlawful sharing of their
18 Personal and Medical Information, including but not limited to time and effort spent researching
19 how to prevent, detect, contest, and recover from fraud and identity theft and implementing measures
20 to do so; and the continued risk to their Personal and Medical Information, which remain in
21 Defendant's possession, custody or control and is subject to further unauthorized disclosures so long
22 as Defendant fails to undertake appropriate and adequate measures to protect the Personal and
23 Medical Information of current and former patients and their beneficiaries and dependents; and (v)
24 present and future costs in terms of time, effort, and money that will be expended to prevent, detect,
25 contest, and repair the impact of the Personal and Medical Information compromised by Defendant's
26 actions.

27 171. But for Defendant's disclosure of Plaintiff's and the Class members' Personal and
28 Medical Information in violation of the parties' understanding and reasonable expectation of

1 confidence, their Personal and Medical Information would not have been compromised, stolen,
2 viewed, accessed, and used by unauthorized third parties. Such actions and inactions were the direct,
3 proximate, and legal cause of the exfiltration of Plaintiff's and Class members' Personal and Medical
4 Information as well as the resulting damages.

5 172. The injury and harm Plaintiff and the Class members suffered was the reasonably
6 foreseeable result of Defendant's conduct, which permitted the unauthorized disclosure of Plaintiff's
7 and Class members' Personal and Medical Information. Defendant either knew, or should have
8 known, that its methods of accepting and securing Plaintiff's and the Class members' Personal and
9 Medical Information was inadequate as it relates to, at the very least, securing servers and other
10 computer equipment solely the responsibility of BetterHelp and containing Plaintiff's and the Class
11 members' Personal and Medical Information.

12 173. As a direct and proximate result of Defendant's breaches of its duties, Plaintiff and
13 Class members have suffered and will suffer injury, including, but not limited to: (i) actual identity
14 compromise; (ii) the loss of the opportunity how their Personal and Medical Information is used;
15 (iii) the compromise and publication of their Personal and Medical Information to unauthorized third
16 parties; (iv) time and expenses associated with the prevention, detection, and recovery from identity
17 theft, tax fraud, or other unauthorized use of their Personal and Medical Information; (v) lost
18 opportunity costs associated with effort expended and the loss of productivity addressing and
19 attempting to mitigate the actual present and future consequences of the unlawful sharing of their
20 Personal and Medical Information, including but not limited to time and effort spent researching
21 how to prevent, detect, contest, and recover from fraud and identity theft and implementing measures
22 to do so; and the continued risk to their Personal and Medical Information, which remain in
23 Defendant's possession, custody or control and is subject to further unauthorized disclosures so long
24 as Defendant fails to undertake appropriate and adequate measures to protect the Personal and
25 Medical Information of current and former patients and their beneficiaries and dependents; and (vi)
26 present and future costs in terms of time, effort, and money that will be expended to prevent, detect,
27 contest, and repair the impact of the Personal and Medical Information compromised by Defendant's
28 actions.

1 174. Plaintiff seeks the award of actual damages on behalf of herself and members of the
2 Class.

3 175. In failing to secure Plaintiff's and Class members' Personal and Medical Information
4 and promptly and fully notifying them of the facts surrounding this data breach and its failure to
5 have in place systems that would protect such data from being compromised, Defendant is guilty of
6 oppression, fraud, and malice. Defendant acted or failed to act with a reckless, willful, or conscious
7 disregard of Plaintiff's and Class members' rights. Plaintiff, in addition to seeking actual damages,
8 also seeks punitive damages on behalf of herself and the Class.

9 176. Plaintiff also seeks injunctive relief on behalf of the Class in the form of an order
10 compelling Defendant to institute appropriate data collection and safeguarding methods and policies
11 with regard to patient information, as set forth below.

12 SEVENTH CLAIM FOR RELIEF

13 Breach of Fiduciary Duty

14 177. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein
15 to the extent relevant to this Claim for Relief and the relief available thereunder.

16 178. Plaintiff and Class members gave Defendant their Personal and Medical Information
17 in confidence, believing that Defendant would protect that information. Plaintiff and Class members
18 would not have provided Defendant with this information had they known it would not be adequately
19 protected.

20 179. Defendant's acceptance and storage of Plaintiff's and Class members' Personal and
21 Medical Information created a fiduciary relationship between Defendant and Plaintiff and Class
22 members. In light of this relationship, Defendant must act primarily for the benefit of its members,
23 which includes safeguarding and protecting Plaintiff's and Class Members' Personal and Medical
24 Information.

25 180. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members
26 upon matters within the scope of their relationship. It breached that duty by failing to properly
27 safeguard Plaintiff's and Class members' Personal and Medical Information that it collected.

28 181. As a direct and proximate result of Defendant's breaches of its duties, Plaintiff and

1 Class members have suffered and will suffer injury, including, but not limited to: (i) actual identity
2 compromise; (ii) the loss of the opportunity how their Personal and Medical Information is used;
3 (iii) the compromise and publication of their Personal and Medical Information to unauthorized third
4 parties; (iv) time and expenses associated with the prevention, detection, and recovery from identity
5 theft, tax fraud, or other unauthorized use of their Personal and Medical Information; (v) lost
6 opportunity costs associated with effort expended and the loss of productivity addressing and
7 attempting to mitigate the actual present and future consequences of the unlawful sharing of their
8 Personal and Medical Information, including but not limited to time and effort spent researching
9 how to prevent, detect, contest, and recover from fraud and identity theft and implementing measures
10 to do so; and the continued risk to their Personal and Medical Information, which remain in
11 Defendant's possession, custody or control and is subject to further unauthorized disclosures so long
12 as Defendant fails to undertake appropriate and adequate measures to protect the Personal and
13 Medical Information of current and former patients and their beneficiaries and dependents; and (vi)
14 present and future costs in terms of time, effort, and money that will be expended to prevent, detect,
15 contest, and repair the impact of the Personal and Medical Information compromised by Defendant's
16 actions.

17 **EIGHTH CLAIM FOR RELIEF**

18 **Breach of Implied Contract**

19 182. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully
20 set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder.

21 183. In connection with receiving medical treatment or other services, Plaintiff and all
22 other Class members entered into implied contracts with BetterHelp. Such an implied contract is
23 established by BetterHelp's conduct, which evidences its intent to enter into an agreement to protect
24 Plaintiff's and Class members Personal and Medical Information.

25 184. The protection of Personal and Medical Information was a material term of the
26 implied contracts between Plaintiff and Class members, on the one hand, and BetterHelp, on the
27 other hand.

28 185. Plaintiff and Class members performed their obligations under the implied contract

1 when they provided BetterHelp with their Personal and Medical Information and paid for services
2 from BetterHelp.

3 186. BetterHelp breached its obligations under its implied contracts with Plaintiff and
4 Class members in failing to implement and maintain reasonable security measures to protect and
5 secure their Personal and Medical Information and in failing to implement and maintain security
6 protocols and procedures to protect Plaintiff's and Class members' Personal and Medical
7 Information in a manner that complies with applicable laws, regulations, and industry standards.

8 187. BetterHelp's breach of the obligations of its implied contracts with Plaintiff and Class
9 members directly resulted in the injuries that Plaintiff and all other Class members have suffered.

10 188. Plaintiff and all other Class members were damaged by as a result of BetterHelp's
11 breach of implied contracts. Those injuries and damages include, but are not limited to: (i) actual
12 identity theft or compromise; (ii) the loss of the opportunity how their Personal and Medical
13 Information is used; (iii) the compromise, publication, and theft of their Personal and Medical
14 Information; (iv) time and expenses associated with the prevention, detection, and recovery from
15 identity theft, tax fraud, and fraud, unwanted and harassing telephone calls, signing up for credit
16 monitoring and credit freezes to redress the unauthorized use of their Personal and Medical
17 Information; (v) lost opportunity costs associated with effort expended and the loss of productivity
18 addressing and attempting to mitigate the actual present and future consequences of this
19 unauthorized disclosure, including but not limited to time and effort spent researching how to
20 prevent, detect, contest, and recover from fraud and identity theft and implementing measures to do
21 so; and the continued risk to their Personal and Medical Information, which remain in Defendant's
22 possession, custody or control and is subject to further unauthorized disclosures so long as Defendant
23 fails to undertake appropriate and adequate measures to protect the Personal and Medical
24 Information of current and former patients and their beneficiaries and dependents; and (vi) present
25 and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest,
26 and repair the impact of the Personal and Medical Information compromised by Defendant's actions.

NINTH CLAIM FOR RELIEF

Unjust Enrichment

1
2
3 189. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein
4 to the extent relevant to this Claim for Relief and the relief available thereunder.

5 190. Defendant benefited from receiving Plaintiff’s and Class members’ Personal and
6 Medical Information by its ability to retain and use that information for its own benefit. Defendant
7 understood the receipt of such monetary benefits included being able to bill for and profit from the
8 use of such services by Plaintiff and Class members that required providing such information to
9 obtain such services, as well as the retention by Defendant of excess profits because Defendant
10 obtained money or property as a result of the use and installation of this surreptitious tracking code
11 from third parties.

12 191. Defendant also understood and appreciated that Plaintiff’s and Class members’
13 Personal and Medical Information was private and confidential, and its value depended upon
14 Defendant maintaining the privacy and confidentiality of that information.

15 192. Defendant failed to expend the resources necessary to provide reasonable security,
16 safeguards, and protections to the Personal and Medical Information of Plaintiff and Class members.

17 193. Under the principles of equity and good conscience, Defendant should not be
18 permitted to retain money that have been unjustly obtained and retained as a result of the use of this
19 surreptitious tracking code.

20 194. Defendant wrongfully accepted and retained these benefits to the detriment of
21 Plaintiff and Class members.

22 195. Defendant’s enrichment at the expense of Plaintiff and Class members is and was
23 unjust.

24 196. As a result of Defendant’s wrongful conduct, as alleged above, Plaintiff and Class
25 members are entitled to restitution and disgorgement of all profits, benefits, and other compensation
26 obtained or retained by Defendant, plus interest thereon at the legal rate.

27
28

TENTH CLAIM FOR RELIEF

Violation of California’s Unfair Competition Law

(Cal. Bus. & Prof. Code §§ 17200 *et seq.*)

197. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder, except as to entitlement to and claims for damages, which are not sought in this Claim for Relief.

198. The acts, misrepresentations, omissions, practices, and non-disclosures of Defendant as alleged herein constituted unlawful and unfair business acts and practices within the meaning of Cal. Bus. & Prof. Code §§ 17200, *et seq.*

199. Defendant engaged in “unlawful” business acts and practices in violation of the California statutes set forth above, including Cal. Civ. Code §§ 56.10(a), 56.101, 1798.21, 1798.29 and Article I, § 1 of the California Constitution, the Online Privacy Protection Act, California Business and Professions Code §§ 22575-22579 (“CalOPPA”), the California Invasion of Privacy Act, Cal. Penal Code § 630-632 *et seq.* (“CIPA”), and California Computer Data Access and Fraud Act, Cal. Penal Code § 502 (“CDAFA”). Defendant also violated federal statutes and regulations, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above. Plaintiff reserves the right to allege other violations of law committed by Defendant that constitutes unlawful business acts or practices within the meaning of Cal. Bus. & Prof. Code §§ 17200, *et seq.* The allegations of facts set forth in detail above specifically describe and demonstrate how Defendant’s actions and inactions violated these laws.

200. Defendant has also engaged in “unfair” business acts or practices. There are several tests that determine whether a practice that impacts consumers as compared to competitors is “unfair,” examining the practice’s impact on the public balanced against the reasons, justifications and motives of Defendant. Defendant’s conduct would qualify as “unfair” under any of these standards:

- 1 (a) whether the practice offends an established public policy, which here is whether the
2 practices at issue offend the policies of protecting consumers' Personal and Medical
3 Information by engaging in illegal practices, as reflected in California law and
4 policy set forth above;
- 5 (b) balancing the utility of Defendant's conduct against the gravity of the harm created
6 by that conduct, including whether Defendant's practices caused substantial injury
7 to consumers with little to no countervailing legitimate benefit that could not
8 reasonably have been avoided by the consumers themselves, and causes substantial
9 injury to them; or
- 10 (c) whether the practice is immoral, unethical, oppressive, unscrupulous,
11 unconscionable or substantially injurious to consumers.

12 201. The unfair business practice and harm caused by Defendant's failure to maintain
13 adequate information security procedures and practices, including, but not limited to, failing to take
14 adequate and reasonable measures to ensure its data systems were protected against unauthorized
15 disclosures, failing to properly and adequately educate and train employees, failing to put into place
16 reasonable or adequately protected computer systems and security practices to safeguard patients'
17 Personal and Medical Information, improperly installing code that would permit access to
18 unauthorized persons and thus failing to have adequate privacy policies and procedures in place that
19 did not preserve the confidentiality of the Personal and Medical Information of Plaintiff and the
20 Class members in its possession, and failing to protect and preserve confidentiality of Personal and
21 Medical Information of Plaintiff and Class members against disclosure and release, outweighs the
22 utility of such conduct and such conduct offends public policy, is immoral, unscrupulous, unethical,
23 and offensive, and causes substantial injury to Plaintiff and Class members. The allegations of facts
24 set forth in detail above specifically describe and demonstrate how Defendant's actions and inactions
25 constitute unfair business practices.

26 202. Defendant either knew or should have known that BetterHelp's data security and
27 protection practices were inadequate to safeguard the Personal and Medical Information of Plaintiff
28 and Class members. The business acts and practices by Defendant for failure to keep confidential

1 medical, demographic, or personal data protected, did not meet all applicable standards of care and
2 vigilance.

3 203. These unlawful and unfair business acts or practices conducted by Defendant has
4 been committed in the past and continue. Defendant has failed to acknowledge the wrongful nature
5 of its actions. Defendant has not corrected or publicly issued comprehensive corrective notices to
6 Plaintiff and the Class members and may not have corrected or enacted adequate policies and
7 procedures to protect and preserve confidentiality of medical and personal identifying information
8 of Plaintiff and the Class in its possession.

9 204. As set forth above, Plaintiff and Class members have been injured in fact and lost
10 money or property as a result of Defendant's unlawful and unfair business practices, having lost
11 control over information about them that has a specific inherent monetary value that can be sold,
12 bartered, or exchanged. In addition, Plaintiff and Class members have suffered injury in fact and a
13 loss of money or property by at least the following: (i) suffering unauthorized identity compromise;
14 (ii) the loss of the opportunity how their Personal and Medical Information is used; (iii) the
15 compromise, publication, and theft of their Personal and Medical Information; (iv) time and
16 expenses associated with the prevention, detection, and recovery to redress the and unauthorized use
17 of their Personal and Medical Information; (v) lost opportunity costs associated with effort expended
18 and the loss of productivity addressing and attempting to mitigate the actual present and future
19 consequences; and the continued risk to their Personal and Medical Information, which remain in
20 Defendant's possession, custody or control and is subject to further unauthorized disclosures so long
21 as Defendant fails to undertake appropriate and adequate measures to protect the Personal and
22 Medical Information of current and former patients and their beneficiaries and dependents; and (vi)
23 present and future costs in terms of time, effort, and money that will be expended to prevent, detect,
24 contest, and repair the impact of the Personal and Medical Information compromised by Defendant's
25 actions.

26 205. Plaintiff and Class members have no other adequate remedy of law in that, absent
27 injunctive relief from the Court, Defendant is likely to not fully redress the issues raised by its illegal
28 and unfair business practices. Defendant has not announced any specific changes to its data security

1 infrastructure, processes, or procedures to fix the vulnerabilities in the electronic information
2 security systems and security practices, nor have they provided prompt notice of the circumstances
3 surrounding this practice as required by law. Thus, there is a real, credible threat of future harm
4 either in terms of the continued misuse of the data that Defendant failed to protect.

5 206. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiff seeks an order of this Court for
6 herself, Class members, and for the benefit of the public granting injunctive relief in the form of
7 requiring Defendant to correct its illegal conduct, to prevent Defendant from repeating the illegal
8 and wrongful practices as alleged above and protect and preserve the confidentiality of Personal and
9 Medical Information in Defendant’s possession that has been accessed, downloaded, exfiltrated, and
10 viewed by at least one unauthorized third party (*i.e.*, Meta, Snapchat, Pinterest, etc.) because of
11 Defendant’s illegal and wrongful practices set forth above. Pursuant to Cal. Bus. & Prof. Code §
12 17203, Plaintiff also seeks an order of this Court for equitable and injunctive relief in the form of
13 prohibiting Defendant from continuing to refuse publicly issuing comprehensive direct and
14 corrective notices as well as restitution and restitutionary disgorgement of the monies Defendant
15 saved and made from third party advertisers or platforms in which Plaintiff and Class members have
16 a vested interest and a superior right thereto.

17 207. This action, if successful, will enforce an important right affecting the public interest
18 and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of
19 persons and the general public. Private enforcement is necessary and places a disproportionate
20 financial burden on Plaintiff in relation to Plaintiff’s stake in the matter. Because this case is brought
21 for the purposes of enforcing important rights affecting the public interest, Plaintiff also seek the
22 recovery of attorneys’ fees and costs in prosecuting this action against Defendant under Cal. Code
23 Civ. Proc. § 1021.5 and other applicable law.

24 **ELEVENTH CLAIM FOR RELIEF**

25 **Declaratory Relief**

26 208. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein
27 to the extent relevant to this Claim for Relief and the relief available thereunder.

28 209. A present and actual controversy exists between the parties. Defendant has failed to

1 acknowledge the wrongful nature of its actions, have not sent affected patients adequate data breach
2 notices, nor publicly issued comprehensive corrective notices. Based on its inadequate disclosures
3 to date, there is also no reason to believe that Defendant has taken adequate measures to correct or
4 enact adequate privacy policies and procedures to protect and preserve Plaintiff's and the Class
5 members' Personal and Medical Information in Defendant's possession.

6 210. Plaintiff and the Class members have no other adequate remedy of law in that, absent
7 declaratory relief from the Court, Defendant is likely to not fully remedy the underlying wrong.
8 Declaratory relief can be sought independent of any other causes of action.

9 211. As described above, Defendant's actions have caused harm to Plaintiff and Class
10 members. Further, Plaintiff and Class members are at risk of additional or further harm due to the
11 exposure of their Personal and Medical Information and Defendant's failure to fully address the
12 security failings that lead to such exposure and provide adequate notice thereof.

13 212. Plaintiff and Class members seek an order of this Court for declaratory, equitable,
14 and injunctive relief in the form of an order finding Defendant has failed and continue to fail to
15 adequately protect Plaintiff's and the Class members' Personal and Medical Information from
16 release to unknown and unauthorized third parties, requiring Defendant to correct or enact adequate
17 privacy policies and security measures to protect and preserve Plaintiff's and Class members'
18 Personal and Medical Information in its possession, and requiring Defendant to publicly issue
19 comprehensive corrective notices to Plaintiff, Class members and the public.

20 **PRAYER FOR RELIEF**

21 WHEREFORE, Plaintiff, both individually and on behalf of the Class and for the benefit of
22 the public, pray for orders and judgment in favor of Plaintiff and against Defendant as follows, as
23 may be applicable to the Causes of Action set forth above:

- 24 • Finding that this action satisfies the prerequisites for maintenance as a class action
25 and certifying the Class defined herein;
- 26 • Designating Plaintiff as representatives of the Class and his counsel as Class counsel;
- 27 • Declaring Defendant's conduct in violation of the laws set forth above, including Cal.
28 Civ. Code §§ 56.10(a), 56.101, 1798.21, 1798.29, Cal. Bus. and Prof. Code §§ 17200

1 et seq., Cal.Bus. and Prof. Code §§ 22575-2257, Cal. Penal Code § 630-632 et seq.,
2 Cal. Penal Code § 502 and Article I, § 1 of the California Constitution.

3 An order:

- 4 • prohibiting Defendant from engaging in the wrongful and unlawful acts described
5 herein;
 - 6 • prohibiting Defendant from failing to protect, including through encryption, all data
7 collected through the course of its business operations in accordance with all
8 applicable regulations, industry standards, and federal and state laws;
 - 9 • prohibiting Defendant from refusing to implement and maintain a comprehensive
10 Information Security Program designed to protect the confidentiality and integrity of
11 the Personal and Medical Information of Plaintiff and the Class members;
 - 12 • prohibiting Defendant from refusing to audit, test, and train security personnel
13 regarding any new or modified procedures;
 - 14 • prohibiting Defendant from refusing to establish an information security training
15 program that includes at least annual information security training for all employees,
16 with additional training to be provided as appropriate based upon the employees'
17 respective responsibilities with handling personal identifying information, as well as
18 protecting the personal identifying information of Plaintiff and Class members;
 - 19 • All appropriate actual, compensatory, statutory, punitive, and other forms of damages
20 as appropriate and permitted under the causes of action set forth above;
 - 21 • All appropriate equitable monetary relief, including restitution and restitutionary
22 disgorgement;
 - 23 • Awarding Plaintiff's counsel reasonable attorneys' fees and non-taxable expenses;
 - 24 • Awarding Plaintiff's costs;
 - 25 • Awarding pre- and post-judgment interest at the maximum rate permitted by
26 applicable law; and,
 - 27 • Granting such further relief as the Court deems just.
- 28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all issues so triable.

Dated: March 11, 2023

DOYLE APC

By: Chris W. Cantrell

William J. Doyle (SBN 188069)

bill@doyleapc.com

Chris W. Cantrell (SBN 209874)

chris@doyleapc.com

DOYLE APC

550 West B St, 4th Floor

San Diego, CA 92101

Phone: (619) 736-0000

Alan M. Mansfield (SBN 125998)

amansfield@whatleykallas.com

WHATLEY KALLAS LLP

1 Sansome Street, 35th Floor, PMB #131

San Francisco, CA 94104 /

16870 West Bernardo Dr., Ste. 400

San Diego, CA, 92127

Phone: (619) 308-5034

Fax: (888) 341-5048

April M. Strauss (SBN 163327)

astrauss@sfaclp.com

APRIL M. STRAUSS, A PC

2500 Hospital Drive, Bldg 3

Mountain View, CA 94040

Phone: (650) 281-7081

Attorneys for Plaintiff