

**KESSLER TOPAZ
MELTZER & CHECK, LLP**
Jennifer L. Joost (Bar No. 296164)
jjoost@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Facsimile: (415) 400-3001

-and-

**KESSLER TOPAZ
MELTZER & CHECK, LLP**
Joseph H. Meltzer
jmeltzer@ktmc.com
Melissa L. Yeates
myeates@ktmc.com
Tyler S. Graden
tgraden@ktmc.com
Jordan E. Jacobson
jjacobson@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

Counsel for Plaintiffs and the proposed Classes
(Additional Attorneys Listed on Signature Page)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

JOHN DOE and JANE DOE, Individually and
on behalf of all others similarly situated,

Plaintiffs,

v.

KAISER FOUNDATION HEALTH PLAN,
INC., KAISER FOUNDATION HOSPITALS,
and THE PERMANENTE MEDICAL GROUP,
INC.,

Defendants.

Case No. 4:23-cv-02865

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

I.	NATURE OF THE ACTION	1
II.	THE PARTIES	4
A.	Plaintiffs	4
1.	Plaintiff John Doe.....	4
2.	Plaintiff Jane Doe	5
B.	Defendants.....	5
III.	JURISDICTION AND VENUE.....	7
IV.	FACTUAL ALLEGATIONS	7
A.	Kaiser Permanente Communicates with Kaiser Plan Members Through the Kaiser Permanente Website.....	7
B.	Multiple Third Party Wiretappers Intercept Kaiser Plan Members’ Information Shared with, and Communications with, Kaiser Permanente and Its Providers	14
1.	Kaiser Permanente Allows Quantum Metric to Intercept Kaiser Plan Members’ Information and Communications	14
2.	Kaiser Permanente Allows Adobe to Intercept Kaiser Plan Members’ Information and Communications	20
3.	Kaiser Permanente Allows Twitter, Bing, and Google to Intercept Patients’ Communications.....	32
C.	Plaintiffs and Class Members Did Not Consent to Kaiser Permanente Disclosure of Their Information and Communications to Third Parties.....	47
D.	Plaintiffs’ and Class Members’ Health Information Has Actual, Measurable, Monetary Value	48
E.	Kaiser Permanente’s Conduct Violates State and Federal Privacy Laws	48
V.	TOLLING.....	52
VI.	CLASS ACTION ALLEGATIONS.....	53
VII.	CLAIMS FOR RELIEF.....	55
VIII.	PRAYER FOR RELIEF	78

Plaintiffs¹ John Doe and Jane Doe bring this proposed class action against Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The Permanente Medical Group, Inc. (collectively “Kaiser Permanente” or “Defendants”), individually and on behalf of all others similarly situated, upon personal knowledge as to Plaintiffs’ own conduct, and on information and belief as to all other matters based on investigation by counsel.²

I. NATURE OF THE ACTION

1. As any reasonable patient would expect, Plaintiffs trusted that their medical providers would treat the information that they shared with them as private and confidential.

2. This expectation extends to Plaintiffs’ use of Kaiser Permanente’s websites, on which they and other patients schedule appointments, access medical test results, learn about treatment options, order and review prescriptions, exchange messages and healthcare information with providers, participate in online health assessments, pay bills, and research specialists, among other sensitive activities.

3. Notwithstanding, Plaintiffs’ and other patients’ reasonable expectation that their interactions and communications through Kaiser Permanente’s website would not be shared with third parties, Kaiser Permanente discloses the contents of patients’ confidential information and communications with a number of third parties, completely unbeknownst to Plaintiffs and its other patients, while those communications are in transit between Plaintiffs and Class Members on the one hand and Kaiser Permanente on the other.

4. Specifically, unbeknownst to Plaintiffs and its other patients, Kaiser Permanente has installed code from multiple third parties throughout the Kaiser Permanente website that allows third

¹ Plaintiffs seek to proceed anonymously, as other plaintiffs have in other litigation claiming privacy violations involving health care providers. *See, e.g.*, Class Action Complaint & Demand for Jury Trial, *Doe v. Meta Platforms Inc.*, No. 22-cv-3580 (N.D. Cal. June 17, 2022), ECF No. 1; Class Action Complaint & Demand for Jury Trial, *Doe v. Meta Platforms Inc.*, No. 22-cv-04680 (N.D. Cal. Aug. 15, 2022), ECF No. 1; Complaint, *Doe v. Meta Platforms Inc.*, No. 22-cv-4963 (N.D. Cal. Aug. 30, 2022), ECF No. 1; Class Action Complaint & Demand for Jury Trial, *Doe v. Meta Platforms Inc.*, No. 22-cv-6665 (N.D. Cal. Oct. 28, 2022), ECF No. 1; Complaint, *Doe v. Meta Platforms Inc.*, No. 22-cv-4293 (N.D. Cal. July 25, 2022), ECF No. 1. Plaintiffs are seeking Defendants’ consent to proceed anonymously.

² Counsel’s investigation includes an analysis of publicly available information. Plaintiffs believe that a reasonable opportunity for discovery will provide further support for the claims alleged herein.

1 party companies such as Quantum Metric, Twitter, Adobe, Bing, and Google (collectively, “Third
2 Party Wiretappers”) to intercept the content of Plaintiffs and Class Members’ patient status,
3 identifying information, medical topics researched, choices made, information shared and
4 communications with their medical providers, including personally identifiable medical information
5 and other confidential information and communications, when that information is in transit.

6 5. The third party code that Kaiser Permanente has installed on its website transmits and
7 redirects the content of Plaintiffs and other Class Members’ communications to these Third Party
8 Wiretappers from the very moment that a user first loads Kaiser Permanente’s website and continues
9 as the user navigates through the website researching and sharing sensitive information.

10 6. Once the website loads, the Third Party Wiretappers continue to intercept the content
11 of patients’ communications with Kaiser Permanente in real time as the patient navigates the website
12 to access specific medical information, clicks buttons that divulge sensitive and protected patient
13 status, and personal and health information, and enters information into various fields on Kaiser
14 Permanente’s website, such as: (1) signing-up for a patient Portal; (2) signing-in or signing-out of a
15 patient portal; (3) taking actions inside a patient Portal; (4) making, scheduling, or participating in
16 appointments; (5) reviewing and ordering prescriptions; (6) exchanging communications relating to
17 doctors, treatments, payment information, health insurance information, prescription drugs,
18 prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; and
19 (7) providing other information that qualifies as “personal health information” and/or identifying
20 information under federal and state laws.

21 7. Kaiser Permanente knew that by embedding the Third Party Wiretappers’ code, they
22 were disclosing and permitting these Third Party Wiretappers to intercept and collect information
23 shared by its website users, including the content of Plaintiffs and Class Members’ communications,
24 which include identifying information, personal and sensitive information relating to medical
25 treatment, and/or information that Kaiser Permanente was required to protect under the Health
26 Insurance Portability and Accountability Act of 1996 (“HIPAA”), 42 U.S.C. § 1320d-6.

8. In fact, in December 2022, the United States Department of Health and Human Services (“HHS”) issued a bulletin “to highlight the obligations” of health care providers under the HIPAA Privacy Rule “when using online tracking technologies” such as those used by Kaiser Permanente which “collect and analyze information about how internet users are interacting with a regulated entity’s website or mobile application.”³

9. In the bulletin, HHS confirmed that HIPAA applies to health care providers’ use of tracking technologies like those developed by the Third Party Wiretappers and used by Kaiser Permanente. Among other things, HHS explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual’s identifying information even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

How do the HIPAA Rules apply to regulated entities’ use of tracking technologies?

Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity’s website or mobile app, including individually identifiable health information (IIHI) that the individual provides when they use regulated entities’ websites or mobile apps. This information might include an individual’s medical record number, home or email address, or dates of appointments, as well as an individual’s IP address or geographic location, medical device IDs, or any unique identifying code. **All such IIHI collected on a regulated entity’s website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.** This is because, when a regulated entity collects the individual’s IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual’s past, present, or future health or health care or payment for care.

10. HHS further clarified that HIPAA applies to health care providers’ webpages with tracking technologies even on webpages that do not require patients to login:

Tracking on unauthenticated webpages

³ Press Release, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS (Dec. 1, 2022), <https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html>; *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, HHS (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

[T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal . . . [and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. **For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider.** In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

11. This HHS bulletin did not create any new obligations, but instead highlights obligations that have been in place for decades, with which Kaiser Permanente should have been complying.

12. Kaiser Permanente's disclosure of patients' patient status, identifying information, and personal and sensitive health information to the Third Party Wiretappers, including without adequate disclosure of its conduct to Plaintiffs and Class Members, constitutes an egregious invasion of Plaintiffs and Class Members' privacy and violates the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; Cal. Const. art. I, § 1; the Washington Privacy Act, Wash. Rev. Code § 9.73, *et seq.*; Washington Health Care Act, Wash. Rev. Code § 70.02.005, *et seq.*, and HIPAA, and constitutes intrusion upon seclusion and breach of Kaiser Permanente's express and implied promises and duties to its patients, including Plaintiffs and members of the Classes.

II. THE PARTIES

A. Plaintiffs

1. Plaintiff John Doe

13. Plaintiff John Doe is a citizen of California, and resides in Victorville, California.

14. Plaintiff John Doe is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since in or around 2012.

1 15. Plaintiff John Doe regularly uses Kaiser Permanente's website and Patient Portal to
2 access medical information and communicate with his health care providers, including making
3 appointments, reviewing and ordering prescriptions, researching providers and medical conditions,
4 communicating with providers, checking medical results, and reviewing his medical history.

5 16. Without Plaintiff John Doe's knowledge or consent, Kaiser Permanente allowed the
6 Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or
7 meaning of the contents of his patient status, identifying information, personal and sensitive health
8 information, and confidential communications with his health care providers through Kaiser
9 Permanente's website while that information and those messages, reports, and/or communications
10 were in transit.

11 **2. Plaintiff Jane Doe**

12 17. Plaintiff Jane Doe is a citizen of Washington, and resides in Everett, Washington.

13 18. Plaintiff Jane Doe is a Kaiser Foundation Health Plan member and has received
14 medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since
15 2018.

16 19. Plaintiff Jane Doe regularly uses Kaiser Permanente's website and Patient Portal to
17 access medical information and communicate with her health care providers, including making
18 appointments, researching providers and medical conditions, checking medical results, and reviewing
19 her medical history.

20 20. Without Plaintiff Jane Doe's knowledge or consent, Kaiser Permanente allowed the
21 Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or
22 meaning of the contents of her patient status, identifying information, personal and sensitive health
23 information, and confidential communications with her health care providers through Kaiser
24 Permanente's website while that information and those messages, reports, and/or communications
25 were in transit.

26 **B. Defendants**

27 21. Defendant Kaiser Foundation Health Plan, Inc. is a health care provider headquartered
28 in Oakland, California.

1 22. Kaiser Foundation Health Plan, Inc. has an integrated care model, offering both
2 hospital and physician care through a network of hospitals and physician practices operating under
3 the Kaiser Permanente name. Members of Kaiser Permanente health plans have access to hospitals
4 and hundreds of other health care facilities operated by Kaiser Foundation Hospitals and Permanente
5 Medical Groups across the United States.

6 23. Kaiser Foundation Health Plan, Inc. is financially responsible for the payment of
7 medical services provided to its enrollees (“Kaiser Plan Members”) or has accepted such financial
8 responsibility under contract with one or more of the Kaiser Permanente entities. Kaiser Foundation
9 Health Plan, Inc. is the largest health care service plan in the United States, with over 11.8 million
10 members in eight states (California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia, and
11 Washington) and the District of Columbia.

12 24. Kaiser Foundation Hospitals is a non-profit, public-benefit corporation headquartered
13 in Oakland, California. Kaiser Foundation Hospitals operates nearly 40 acute care hospitals and 680
14 medical offices in eight states (California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia,
15 and Washington) and Washington D.C., with its largest presence being in California, where the
16 majority of its hospitals are located, and a significant presence in Washington with more than 35
17 facilities throughout Western Washington and the Spokane area. Kaiser Foundation Hospitals
18 employs more than 21,000 physicians, representing all medical fields.

19 25. The Permanente Medical Group, Inc. is headquartered in Oakland, California and is
20 comprised of physician-owned, for-profit, partnerships, and professional corporations.

21 26. Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The
22 Permanente Medical Group, Inc. operate under the name “Kaiser Permanente,” which is not a legal
23 entity but a registered trademark or trade name that Kaiser Foundation Health Plan, Inc. owns and
24 Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The Permanente Medical
25 Group, Inc. use, acting in concert.

III. JURISDICTION AND VENUE

27. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 because this suit is brought under the laws of the United States, specifically the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.* This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because this a proposed class action in which there are at least 100 Class Members, the matter in controversy, exclusive of interest and costs, exceeds the sum or value of \$5,000,000, and a member of the Class is a citizen of a different State than Defendant.

28. This Court also has supplemental jurisdiction over the state common law and statutory claims pursuant to 28 U.S.C. § 1367, as these claims are so related to the federal statutory claims over which this Court has original jurisdiction, that they form part of the same case or controversy.

29. This Court has general personal jurisdiction over Defendants because Defendants have sufficient minimum contacts with this District in that they operate and market their services throughout the region and in this District. Further, this Court has personal jurisdiction over Defendants because Defendants are headquartered in this District.

30. Venue properly lies in this District pursuant to 28 U.S.C. § 1391(a), (b), and (c) because: a substantial part of the events or omissions giving rise to Plaintiffs and the Classes' claims occurred in this District, Defendants conduct a substantial amount of business in this District, and Defendants are headquartered in this District.

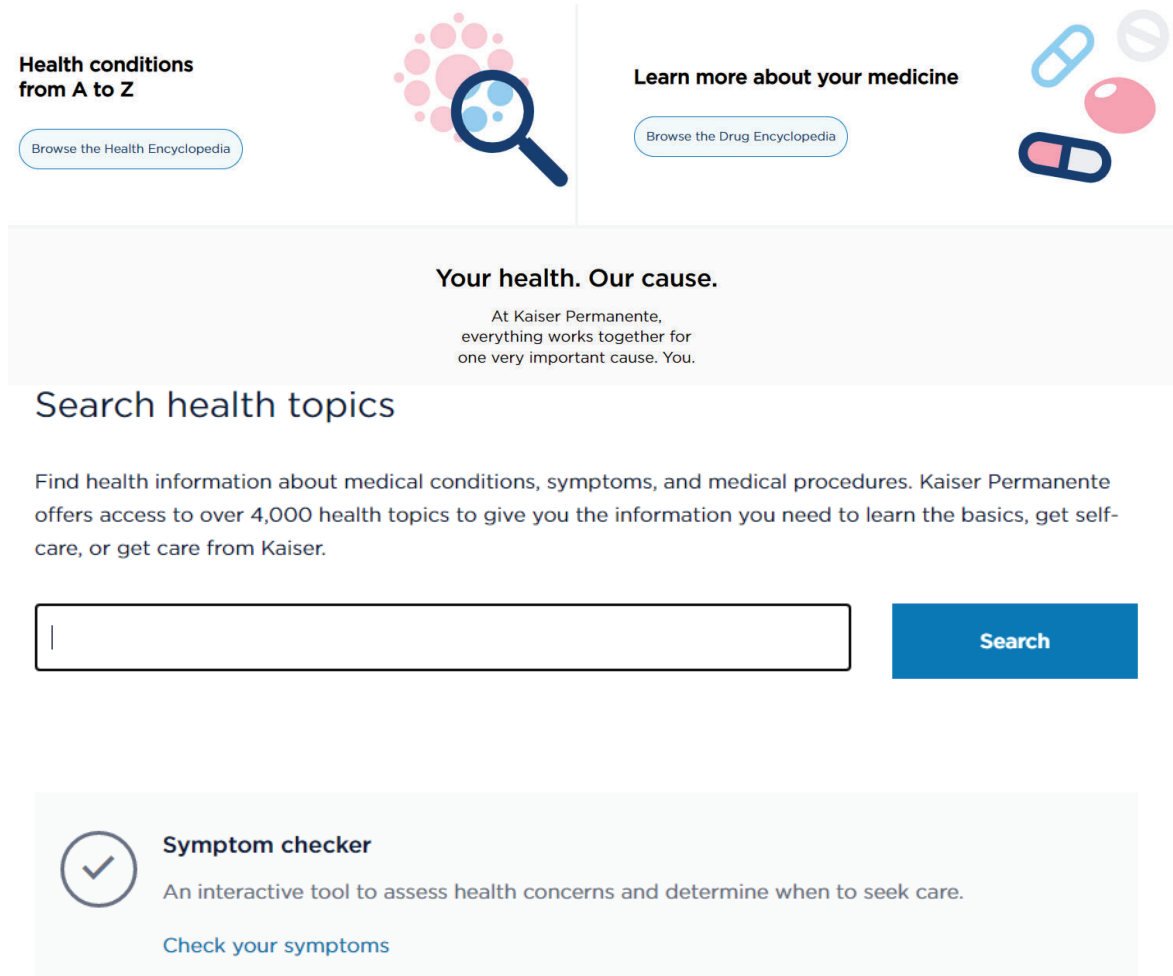
IV. FACTUAL ALLEGATIONS

A. Kaiser Permanente Communicates with Kaiser Plan Members Through the Kaiser Permanente Website

31. Plaintiffs and members of the Classes are Kaiser Plan Members.

32. Kaiser Permanente operates a website ("Site"), with a homepage located at <https://healthy.kaiserpermanente.org/front-door> ("Homepage"), through which Kaiser Plan Members can perform various tasks that traditionally were only available by physically visiting their health care providers' offices or speaking directly to their health care providers, such as scheduling appointments; checking medical results; reviewing medical histories; researching doctors, locations, and medical services; communicating with providers and paying medical bills.

33. The Site's Homepage provides Kaiser Plan Members and the public with information about the health care services that Kaiser Permanente offers, including links to find doctors and locations, get information about health conditions, and learn more about prescribed medicines.



34. For example, on the Homepage, Kaiser Plan Members can click “Browse Health Encyclopedia” and access a page that allows them to find health information about certain medical conditions, symptoms and medical procedures, including over 4,000 health topics, by typing their health-related information into a search form. Kaiser Plan Members can also check their symptoms with an interactive “symptom checker” and “determine when to seek care.”

35. As the Site states, these topics and medical information provide Kaiser Plan Members with the information needed to “learn the basics, get self-care, or get care from Kaiser.”

36. On the Homepage, Kaiser Plan Members can also click “Find a doctors or location” and access a form (<https://healthy.kaiserpermanente.org/southern-california/doctors-locations#/search-form>) where they can input their personal and health information to search for health care providers, including by location, specialty, or provider type or with particular keywords related to medical conditions or symptoms the Kaiser Plan Member is experiencing.

The screenshot displays a search interface with the following elements:

- ENTER ZIP CODE:** A text input field.
- DISTANCE:** A dropdown menu currently showing "WITHIN 10 MILES".
- CITY:** A dropdown menu with the text "Select city".
- OR:** A text label positioned between the "CITY" and "HEALTH PLAN" sections.
- HEALTH PLAN:** A dropdown menu currently showing "Show all plans".
- PROVIDER TYPE:** A dropdown menu currently showing "Show all provider types".
- HOSPITALS, SPECIALTIES, DOCTORS' NAMES, OR KEYWORDS:** A large text input field.
- ENTER SEARCH TERMS:** A label positioned below the large text input field.

37. Kaiser Plan Members can also access their medical information, prescription information and test results, pay bills, schedule appointments, order prescriptions, communicate with providers, and perform other actions related to their healthcare after clicking the “Sign In” Link for their region (“Portal Login Page”) and accessing a purportedly secure patient Portal (the “Portal”). For example, if the Kaiser Plan Member, like Plaintiff John Doe, is located in Southern California, they can select “California – Southern” from a “Region” pulldown menu, click the “Sign In” link and be taken to the Portal Login page for Southern California located at <https://healthy.kaiserpermanente.org/southern-california/consumer-sign-on#/signon>:

Region: California - Southern Language: English

KAISER PERMANENTE Learn Shop Plans Doctors & Locations Health & Wellness Get Care Pay Bills

Sign in

All fields required unless marked as optional.

USER ID

Enter the user ID for your account

PASSWORD

Enter your password for your account

Sign in

[Forgot your User ID or password?](#)

[Register for an account](#)

38. Kaiser Plan Members in Northern California, or other Regions such as Colorado, Georgia, Hawaii, Maryland/Virginia/Washington, D.C., Oregon/ S.W. Washington, and Washington can similarly select their region from a pulldown menu and access their Portal Login Page:

Region: California - Southern Language: English

KAISER PERMANENTE Learn Shop Plans Doctors & Locations Health & Wellness Get Care Pay Bills

Sign in

All fields required unless marked as optional.

USER ID

Enter the user ID for your account

PASSWORD

Enter your password for your account

Sign in

[Forgot your User ID or password?](#)

[Register for an account](#)

39. After signing into the Portal Login Page and entering the Portal, Kaiser Plan Members can access an array of services and view and provide personal and highly sensitive medical information, including viewing medical history, prescriptions, test results, scheduling appointments, performing online medical evaluations, researching symptoms, and communicating with providers, among other things.

40. For example, the Portal contains a “Message Center” that allows Kaiser Plan Members to communicate directly with their health care providers:

Send a message to:

COVID-19 & Flu: How to get care
[Start an e-visit](#) to get online care and advice 24/7 for COVID-19 and flu, request a COVID-19 vaccine or test, or report a positive COVID-19 self-test. To learn more about COVID-19 and treatment options like Paxlovid, visit kp.org/covid.
 For COVID-19 test results, visit [Test Results](#) instead of contacting your doctor's office. Test results are usually available in 1-2 days.

Choose a department to continue.

Selection is required.

☐ **Doctor's office**
 For nonurgent and wellness questions.

☐ **Member services**
 For billing or health plan questions, help setting up your account, or comments about your Kaiser Permanente experience.

☐ **Web assistance**
 For technical problems with the website or suggestions on how to improve it.

41. After selecting a particular department, Kaiser Plan Members can identify specific recipients to whom they choose to communicate with and type out messages in a free form “Messages” box, with replies also sent and received within the Message Center.

Send a message to the care team of

Choose a recipient

What brings you here today?

Select an option

Write your message below (required):

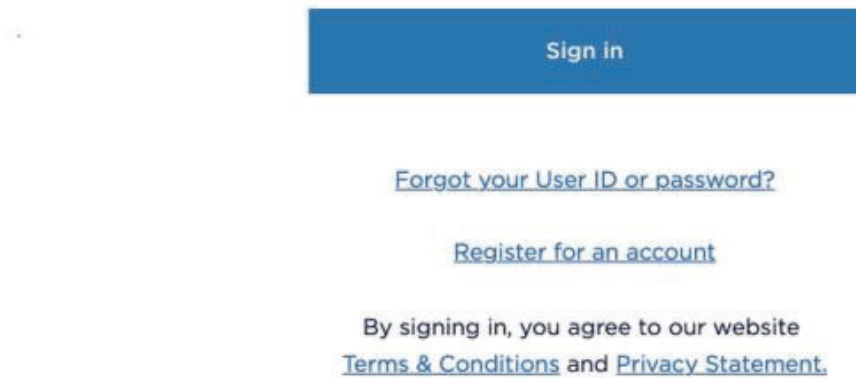
1000 of 1000 characters left

You may attach up to three files (optional). You can send these file types: JPEG, JPG and PDF. The maximum total file size cannot exceed 4.8 megabytes.

[Get more help with attachments.](#) Attachment

Website Feedback

42. The bottom of the Portal Login Page also provides: “By signing in, you agree to our website Terms & Conditions and Privacy Statement.”



43. The Kaiser Permanente Terms & Conditions, available via hyperlink⁴ and attached hereto as Exhibit 1, provides: “Any personal information you submit to the Site (for yourself or someone else) is governed by our Website and KP Mobile Application Privacy Statement.”

44. The Kaiser Permanente Privacy Statement, also available via hyperlink⁵ attached hereto as Exhibit 2, assures Kaiser Plan Members that Kaiser Permanente’s data collection “is

⁴ See, e.g., *Terms & Conditions for our Website and Mobile Application*, Kaiser (Updated Jun. 2022), <https://healthy.kaiserpermanente.org/southern-california/termsconditions>.

⁵ See, e.g., *Website and mobile application Privacy Statement*, Kaiser, <https://healthy.kaiserpermanente.org/southern-california/privacy> (last visited June 9, 2023).

1 collected on an aggregate basis, which means that no personally identifiable information is associated
2 with the data,” which is untrue.

3 45. The Kaiser Permanente Privacy Statement also states that Kaiser Permanente and its
4 service providers may place “cookies” or similar technologies on the computer hard drives of visitors
5 to the Site, but falsely states that information obtained from cookies is only used to help Kaiser
6 Permanente “tailor our Site to be more helpful and efficient for our visitors” when in fact the cookies
7 are also being used for marketing purposes, unbeknownst to Kaiser Plan Members and without their
8 permission or agreement.

9 46. The Kaiser Permanente Privacy Statement also falsely states that “[t]he cookie
10 consists of a unique identifier that does not contain information about your health history,” when in
11 fact the information provided to the Third Party Wiretappers contains information about Kaiser Plan
12 Members’ health history.

13 47. The Kaiser Permanente Privacy Statement also states that Kaiser “may also
14 occasionally use ‘Web beacons’ (also known as ‘clear gifs,’ ‘Web bugs,’ ‘1-pixel gifs,’ etc.)” but
15 falsely claims that Kaiser Permanente does “not collect any personal health information.”

16 48. The Kaiser Permanente Privacy Statement also does not disclose to Kaiser Plan
17 Members that Kaiser Permanente has aided, agreed with, employed, and/or conspired with, third
18 parties that are recording the information that Kaiser Plan Members are sending, accessing,
19 reviewing, or receiving through the Site.

20 49. Kaiser Permanente’s website also contains a HIPAA Notice of Privacy Practices,⁶
21 which purports to describe how and when Kaiser Permanente discloses information covered by
22 HIPAA; however, nowhere in the HIPAA Notice of Privacy Practices does Kaiser Permanente
23 disclose that it is providing HIPAA-protected and other confidential information to the Third Party
24 Wiretappers.

25 50. Kaiser Permanente expressly and impliedly promises Kaiser Plan Members that it will
26 maintain the privacy and confidentiality of the information shared, and the communications engaged

27 ⁶ See, e.g., *Notice of Privacy Practices*, Kaiser, [https://healthy.kaiserpermanente.org/southern-](https://healthy.kaiserpermanente.org/southern-california/privacy-practices)
28 [california/privacy-practices](https://healthy.kaiserpermanente.org/southern-california/privacy-practices) (last visited June 9, 2023).

1 in, on the Site and the Portal and that such information and communications will not be disclosed to
2 or tracked by third parties.

3 51. Despite its express and implied assurances of privacy, Kaiser Permanente intentionally
4 incorporated the Third Party Wiretappers' code and recording technology on the Kaiser Permanente
5 website, and allowed the tracking and disclosure of Kaiser Plan Members' identifying information,
6 personal and sensitive health information, and private, sensitive, and confidential communications
7 with Kaiser Permanente and its providers to Third Party Wiretappers.

8 **B. Multiple Third Party Wiretappers Intercept Kaiser Plan Members' Information**
9 **Shared with, and Communications with, Kaiser Permanente and Its Providers**

10 **1. Kaiser Permanente Allows Quantum Metric to Intercept Kaiser Plan**
11 **Members' Information and Communications**

12 52. Unbeknownst to Kaiser Plan Members and against their reasonable expectations,
13 Kaiser Permanente allows Quantum Metric to intercept Kaiser Plan Members' personal and sensitive
14 identifying and medical information and confidential communications from the Site and Portal.

15 53. Kaiser Permanente has placed Quantum Metric's "Session Replay" code on its
16 Homepage, Portal Login Page, and other pages on the Site—including within the Portal—which
17 intercepts and records the contents of Kaiser Plan Members' information and confidential
18 communications, and sends that information and those communications to Quantum Metric.

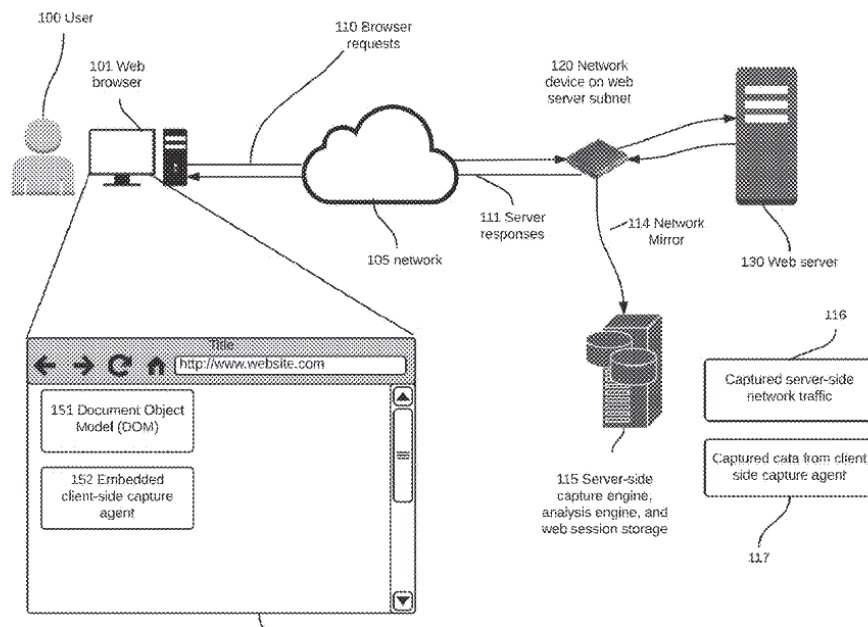
19 54. Quantum Metric collects and saves website communications, including those on the
20 Site and Portal, through a service named "Session Replay." Session Replay captures internet
21 communications between a website user and a website, including those on the Site and Portal, in real
22 time while those communications are in transit.

23 55. As Quantum Metric explains: "At its core, **session replay** is technology that allows
24 you to watch an end user's session as they experienced it, similar to how you watch a video. You can
25 pause, rewind, and fast-forward the session (just like a YouTube video) to watch how a user interacts
26 with a website or mobile app."⁷

27 ⁷ *What is Session Replay*, Quantum Metric, <https://www.quantummetric.com/enterprise-guide-to-session-replay> (last visited June 9, 2023).
28

56. Session replay technologies work by using “embedded snippets of code . . . [that] watch and record a visitor’s every move on a website, in real time.”⁸ This was done on the Site and the Portal when used by Kaiser Plan Members.

57. As illustrated in Quantum Metric’s patent, after a user submits a communication to a web server, such as Kaiser Permanente’s, Quantum Metric’s embedded side capture agent code redirects the communications to Quantum Metric’s server-side capture engine, analysis engine, and web session storage:



58. From the moment a Kaiser Plan Member loads Kaiser Permanente’s website, Quantum Metric is intercepting all of the content viewed and communicated, as well as the Kaiser Plan Member’s interactions with the website, similar to an individual peering over the user’s shoulder and listening in on the patient’s conversations with their medical provider.

59. As Kaiser Plan Members navigate the Kaiser Permanente Site, including accessing the Portal, the Site makes numerous “POST” calls to Quantum Metric, the size of which change based on site activity. A “POST” call is a HTTP method that sends user data to a server.

⁸ Tomas Foltyn, *What’s the Deal with Session-Replay Scripts?*, welivesecurity (Apr. 20, 2018, 1:40 pm), <https://www.welivesecurity.com/2018/04/20/whats-deal-session-replay-scripts/>.

1 60. Thus, by installing the Quantum Metric Replay code on its website, Kaiser
2 Permanente allowed Quantum Metric to intercept and record Kaiser Plan Members' identifying
3 information, personal and sensitive medical information, including HIPAA-protected health
4 information, and confidential communications with Quantum Metric's Session Replay code, in real
5 time.

6 61. On information and belief, Kaiser Permanente has been continually allowing Third
7 Party Wiretappers to intercept Kaiser Plan Member's personal information.

8 62. By way of example, on May 31, 2023, after Plaintiff Jane Doe logged into the Portal—
9 which displayed her Name, Medical Record Number (Kaiser ID #), Region, and Coverage Status—
10 but performed no further activities, the amount of data intercepted and transferred to Quantum Metric
11 (at kp-app.quantummetric.com) was about 260 bytes. Thereafter, when Plaintiff performed several
12 activities within the Portal, the amount of the data transferred to Quantum Metric increased to over
13 102 kB, indicating that her activity inside the Portal was being intercepted by Quantum Metric and
14 redirected to kp-app.quantummetric.com.

15 63. After Plaintiff Jane Doe logged into the Portal and then accessed the Doctor Search
16 Page and performed no further activities, the amount of data intercepted and transferred to Quantum
17 Metric was 311 bytes. Thereafter, when Plaintiff Jane Doe entered personal medical search
18 information into the Doctor Search page, the amount of data transferred to Quantum Metric increased
19 to over 122 kB, indicating that Plaintiff Jane Doe's medical search information was being intercepted
20 by Quantum Metric and redirected to kp-app.quantummetric.com. Kaiser Permanente allowed
21 Quantum Metric to intercept similar information from Jane Doe in the months and years proceeding
22 her logging in on May 31, 2023, and similarly allowed Quantum Metric to intercept log-in
23 information for Plaintiff John Doe and other members of the Classes.

24 64. On June 6, 2023, when Plaintiff John Doe logged into the Portal and accessed recent
25 medical test results, the amount of data transferred to Quantum Metric was over 85 kB, indicating
26 that information about Plaintiff John Doe's personal and sensitive identifying and medical
27

1 information, and private and confidential medical test results, was also being intercepted by Quantum
2 Metric and redirected to kp-app.quantummetric.com.

3 65. On information and belief, the same type of information tracked, disclosed, and sent
4 to Quantum Metric for Plaintiffs has been tracked, disclosed, and sent to Quantum Metric for other
5 members of the Classes.

6 66. Additionally, when Kaiser Plan Members navigate other portions of the Site, Quantum
7 Metric intercepts and receives that content as well. For example, if a patient searches for doctors who
8 specialize in Addiction Medicine, Quantum Metric will receive the search results displaying this
9 sensitive information, as well as data regarding all of the information the Kaiser Plan Members
10 provided and received regarding that topic.

11 67. In addition, when Plaintiff Jane Doe accessed her bill pay account, the amount of data
12 transferred to Quantum Metric was over 84 kB, indicating that information about Plaintiff Jane Doe's
13 personal and sensitive identifying health related financial information was also being intercepted by
14 Quantum Metric and redirected to kp-app.quantummetric.com.

15 68. When Plaintiff John Doe participated in a Social Health Review inside the Portal the
16 amount of data transferred to Quantum Metric was over 25 kB, indicating that information about
17 Plaintiff John Doe's personal and sensitive identifying and medical information, and private and
18 confidential medical test results, was also being intercepted by Quantum Metric and redirected to kp-
19 app.quantummetric.com.

20 69. When Plaintiff John Doe accessed the Message Center inside the Portal, the amount
21 of data transferred to Quantum Metric was over 330.7 kB, indicating that information about Plaintiff
22 John Doe's personal and sensitive identifying and medical information, and private and confidential
23 medical test results, was also being intercepted by Quantum Metric and redirected to kp-
24 app.quantummetric.com.

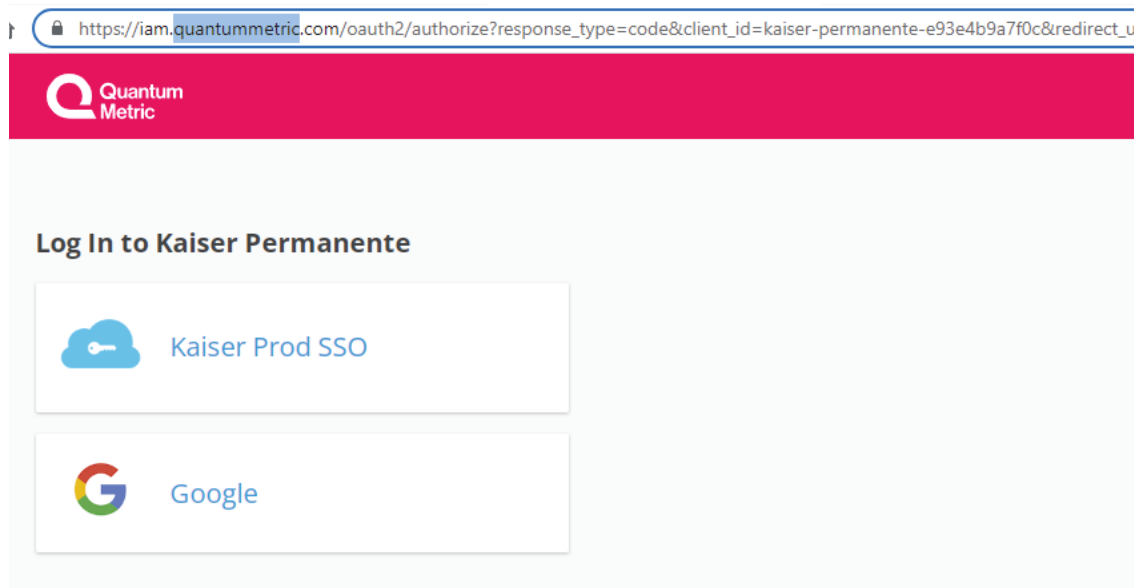
25 70. When Plaintiff John Doe accessed his Medical Summary inside the Portal, the amount
26 of data transferred to Quantum Metric was over 25 kB, indicating that information about Plaintiff
27 John Doe's personal and sensitive identifying and medical information, and private and confidential
28

1 medical test results, was also being intercepted by Quantum Metric and redirected to kp-
2 app.quantummetric.com.

3 71. When Plaintiff John Doe accessed his bill pay account, the amount of data transferred
4 to Quantum Metric was over 84 kB, indicating that information about Plaintiff John Doe's personal
5 and sensitive identifying health related financial information was also being intercepted by Quantum
6 Metric and redirected to kp-app.quantummetric.com.

7 72. When Plaintiff John Doe logged out of the Portal and conducted a search for a
8 neurologist on the Site, the amount of data transferred to Quantum Metric was over 427.1 kB,
9 indicating that information about Plaintiff John Doe's personal and sensitive identifying and medical
10 information, and private and confidential medical test results, was also being intercepted by Quantum
11 Metric and redirected to kp-app.quantummetric.com.

12 73. The recordings of Plaintiffs and other Class Members' information and confidential
13 communications on the Site are saved on Quantum Metric's systems and are available for viewing
14 on Quantum Metric's website, an example of which is below:



24 74. Kaiser Permanente voluntarily embedded Quantum Metric's software code on the
25 Site, knowing that Quantum Metric's software would intercept, record, and redirect Kaiser Plan
26 Members' Site and Portal activity, including personal health information and/or HIPAA-protected
27 information and communications with Kaiser Permanente and its providers.
28

1 75. Unlike certain other third parties, Quantum Metric does not only receive website
 2 analytics data that provides aggregate statistics; rather, the Quantum Metric recording technology
 3 utilized by Kaiser Permanente is intended to record and playback individual browsing sessions, as
 4 well as the private and confidential information and communications shared in those sessions. The
 5 monitoring that Quantum Metric’s technology provides extends beyond the computer “cookies” with
 6 which ordinary consumers may be familiar.

7 76. Moreover, the collection and storage of Kaiser Plan Members’ communications with
 8 their health care providers may cause sensitive health information and other personal information
 9 displayed on a page to leak to additional third parties. This may expose Kaiser Plan Members who
 10 use the Site and/or Portal to identity theft, online scams, and other unwanted behavior.

11 77. In a 2017 study by Princeton University’s Center for Information Technology Policy
 12 concerning session recording technologies, the researchers noted “[c]ollection of page content by
 13 third-party replay scripts may cause sensitive information such as medical conditions, credit card
 14 details and other personal information displayed on a page to leak to the third-party as part of the
 15 recording. This may expose users [like Plaintiffs and members of the Classes] to identity theft, online
 16 scams, and other unwanted behavior.”⁹

17 78. The study goes on to state that “the extent of data collected by these services far
 18 exceeds user expectations; text typed into forms is collected before the user submits the form, and
 19 precise mouse movements are saved, all without any visual indication to the user. This data can’t
 20 reasonably be expected to be kept anonymous.”¹⁰

21 79. As currently deployed, Quantum Metric’s recording function, as employed by Kaiser
 22 Permanente, functions as a wiretap, and Quantum Metric acts as a third-party wiretapper.

23
 24
 25
 26 _____
 27 ⁹ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom
 28 to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

¹⁰ *Id.*

1 **2. Kaiser Permanente Allows Adobe to Intercept Kaiser Plan Members’**
 2 **Information and Communications**

3 80. Unbeknownst to Kaiser Plan Members and against their reasonable expectations,
 4 Kaiser Permanente allows Adobe to intercept Kaiser Plan Members’ information and
 5 communications from the Site and Portal.

6 81. Kaiser Permanente allows Adobe to intercept Kaiser Plan Members’ personal and
 7 sensitive identifying and medical information and private and confidential communications through
 8 code connected with the Adobe Experience Cloud a/k/a Adobe Marketing Cloud service embedded
 9 on the Site, including within the Portal.

10 82. The Adobe Experience Cloud service is a suite of products offered by Adobe, which
 11 allow businesses to personalize and improve their marketing on websites, apps, and social media
 12 pages by collecting and analyzing information about website visitors.

13 83. The Adobe Experience Cloud includes a number of services including: Measurement
 14 solutions, which allows companies to measure and understand visitors who use their websites, apps,
 15 and social media pages, as well as how they interact with online marketing campaigns;
 16 Personalization solutions, which allows companies to test new content and make their websites, apps,
 17 social media pages, and emails more relevant to particular visitors; Content management solutions,
 18 which allows companies to store, update, and deliver images and other content on their websites,
 19 within their apps, and in online marketing materials; and Advertising solutions, which allows
 20 companies to improve their online advertising on websites, apps, search engines, and social media,
 21 including helping companies send emails, text messages, and other online and offline marketing
 22 campaigns.¹¹

23 84. The Adobe Experience Cloud collects an array of information about website visitors,
 24 including:

- 25 • Where you go and what you do on that company’s websites, apps, or social
 26 media pages

27

 28 ¹¹ *Adobe Experience Cloud privacy*, Adobe (Updated Dec. 5, 2022), <https://www.adobe.com/privacy/experience-cloud.html>.

- Your web browsing activity, including the URLs of the company's web pages you visit
- The URL of the page that displayed the link that you clicked on, which brought you to that company's website
- The web search you performed that led you to that company's website
- Information about your web browser and device, such as device type, browser type, advertising identifier, operating system, connection speed, and display settings
- Your IP address (or partial IP address, depending on how the company has configured the solution), which may be used to approximate your general location
- Location information from your mobile device or web browser
- Social media profile information
- Information you may provide on that company's website, app, or when interacting with that company's social media pages, such as information you provide on registration forms
- Ad campaign success rates, such as whether you clicked on a company's ad and whether viewing or clicking on the ad led to your purchase of that company's product or service
- Items you've purchased or placed in your shopping cart on that company's website or app¹²

85. As part of the Adobe Advertising Cloud solution, Adobe makes available certain health-related segments supplied by third-party data providers to the companies using the Adobe Advertising Cloud, allowing companies to use these segments to target ads when they are using the Adobe Experience Cloud. These data segments generally fall into the following categories: (1) occupation in a health related field, (2) health related topics and conditions, (3) interest in health insurance, (4) diet, fitness, weight-loss, and healthy lifestyles, (5) consumer goods and services for personal healthcare, vision care, grooming, and beauty, (6) over the counter medicines, remedies, and dietary supplements, and (7) health related charities.

86. The Adobe Experience Cloud collects this information through an array of tracking technologies, including cookies and/or web beacons (also known as tags or pixels), such as the third

¹² *Id.*

party cookies omtrdc.net, demdex.net, and the Adobe Experience Platform Launch, which delivers a library containing specified tags for other Adobe Experience Cloud solutions.¹³

87. As Kaiser Plan Members navigate the Kaiser Permanente Site, the Site makes numerous “POST” calls which send information about Kaiser Plan Members’ confidential communications with Kaiser Permanente that are intercepted by Adobe.

88. Adobe has established subdomains on its own server, such as the subdomain kaiser.tt.omtrdc.net on Adobe’s omtrdc.net server, where Adobe receives and stores the communications intercepted from Kaiser Permanente.¹⁴

89. For example, on June 6, 2023, after Plaintiff John Doe logged into the Portal, the following data was intercepted by Adobe and sent to Adobe’s server at the kaiser.tt.omtrdc.net subdomain, which as detailed below shows that Adobe received a host of personally identifiable health information, including: user data (color coded in blue), the URL of the Website the user is currently browsing (color coded in green), unique IDs (color coded in yellow), customer IDs and status values (color coded in grey),¹⁵ and segmentation values that enable the Website to show personalized content (no color).

```
{
  "requestId": "d65c5d634b7d484a9176516962af4071",
  "context": {
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36",
    "clientHints": {
      "mobile": false,
      "platform": "macOS",
      "browserUAWi": {
        "majorVersion": "Google Chrome",
        "v": "113",
        "Chromium": "113",
        "NotA.Brand": "24"
      },
      "timeOffsetInMinutes": 420,
      "channel": "web",
      "screen": {
        "width": 1512,
        "height": 982,
        "orientation": "landscape",
        "colorDepth": 30,
        "pixelRatio": 2
      },
      "window": {
        "width": 1512,
        "height": 871
      },
      "browser": {
        "host": "healthy.kaiserpermanente.org",
        "webGLRenderer": "ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)",
        "address": {
          "url": "https://healthy.kaiserpermanente.org/southern-california/secure/inner-door",
          "referrerUrl": "https://healthy.kaiserpermanente.org/southern-california/consumer-interrupt.html"
        }
      },
      "id": {
        "tntId": "Redacted",
        "dPartyId": "Redacted",
        "marketingCloudVisitorId": "Redacted",
        "customerIds": [
          {
            "id": "Redacted",
            "integrationCode": "kpaamid"
          }
        ]
      }
    }
  }
}
```

¹³ This includes cookies identified as “everest_g_v2” and “demdex.net”, which aid in tracking users. According to Adobe’s marketing materials, the everest_g_v2 cookie is “created after a user initially clicks a client’s ad, and used to map the current and subsequent clicks with other events on the client’s website.”

¹⁴ *Adobe Experience Cloud privacy*, supra note 11.

¹⁵ Specific identifier number has been redacted.

epp","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted integrationCode":"kpaamidudr","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted integrationCode":"kpaamid One-off-datasets","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted integrationCode":"pzn_crm","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted integrationCode":"mbox3rdPartyId","authenticatedState":"authenticated","type":"DS"}]],"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"01AFA18961CACA34-2D8CDB5E307D31FB"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:inner-door","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":"urn:kp:prodiem","Seg25":false,"entitlement-446":true,"pLoaded":1,"id":"","profileParameters":{"region":"","Seg2":"12","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"Redacted Seg103v":false}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:inner-door","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":7692006,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg101v":27,"Seg516e":false,"Seg126v":false,"modval":6,"Seg21":100453,"Seg22":"","Seg24":"urn:kp:prodiem","Seg25":false,"entitlement-446":true,"pLoaded":1,"id":"","profileParameters":{"region":"","Seg2":"12","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":7692006,"Seg12":"ACTIVE","Seg101v":27,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"Redacted Seg103v":false}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1686076871023,"execution":3.6},{execution":106.5,"parsing":0.2,"request":{"tls":4.2,"timeToFirstByte":88.8,"download":0.7,"responseSize":1534},"telemetryServerToken":"GRgdNPKF2baxcRHAQqAHqyTPswyQefSCMFGH9GY2aUI=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"2499aa7a302a46319e851646fe207f5f","timestamp":1686076871017}}]}

90. Similarly, when Plaintiff Jane Doe logged into the Portal on May 31, 2023, the following data was intercepted by Adobe and sent to Adobe's server at the kaiser.tt.omtrdc.net subdomain:

```
{ "requestId": "f33def0d509a49e1beb96b320fcae2fd", "context": { "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36", "clientHints": { "mobile": false, "platform": "Windows", "browserUA": "WithMajorVersion": "\\Google Chrome\\;v=\\113\\", "\\Chromium\\;v=\\113\\",
```

```

{"Not-A.Brand":true,"v":24,"timeOffsetInMinutes":
420,"channel":"web","screen":{"width":1366,"height":768,"orientation":"landscape",
"colorDepth":24,"pixelRatio":1},"window":{"width":1349,"height":357},"browser":{
"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Intel, Intel(R) HD Graphics Direct3D11 vs 5 0 ps 5 0, D3D11)"},
"address":{"url":"https://healthy.kaiserpermanente.org/consumer-signon#/signon"},
"referringUrl":"https://healthy.kaiserpermanente.org/washington/front-door"},
"beacon":true,"id":{"tntId":"Redacted","marketingCloudVisitorId":"Redacted"},
"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side",
"supplementalDataId":"75CDF51005725EB2-38AA41AF056F9156"},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1685576844326,
"execution":312.9,"execution":540.4,"parsing":1.1,"request":{"tls":30.3,"timeToFirstByte":171,
"download":3.5,"responseSize":1323},"telemetryServerToken":"GRgdNPKF2baxcRHAQqAHq1m+lb9PISy9OC4JmXflkxk=",
"mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},
"requestId":"57f7290ecb644e209d081d8859b9dcb3","timestamp":1685576843853}]}},
"notifications":[{"id":"5aed303df02141b3a56280a73c83f7b3","type":"display",
"timestamp":1685576849764,"parameters":{"Seg18v":"","Seg17v":"","Seg55v":"Logged Out",
"Seg181v":"","Seg81v":"kporg:consumer-signon","Seg14vcookie":"","reEnable":"","throttle-area":""},
"profileParameters":{"region":"","Seg2":"23"},"view":{"name":"signon"}}}],
"impressionId":"c1f577b2a5494fd3a0c74f9e6e4ef092"}

```

91. The first block color coded in blue is sent as part of the HTTP request header and is used to create a digital fingerprint for the specific user by collecting information about the specific user's browser and device information, including details about the user's browser type, computing device, operating system, screen height and width, and details about the user's graphics card. Together these details create a device fingerprint¹⁶ which allows Adobe to compile and track long-term records of the individual's browsing history (and thus deliver targeted advertising or targeted exploits) even when visitors are attempting to avoid tracking—raising a major concern for internet privacy advocates.

92. The second block (green) indicates the URL for the Webpage currently visited by the user. Here, Adobe is receiving information that Plaintiffs logged-into the Portal, signifying that Plaintiffs are Kaiser Plan Members and Kaiser Permanente Patients—information which Kaiser Permanente is prohibited from disclosing under HIPAA and other state and federal laws.

¹⁶ *Fingerprinting*, web.dev, <https://web.dev/learn/privacy/fingerprinting/> (last visited June 9, 2023).

93. The third block (yellow) includes two identifiers set by Adobe: (1) marketingCloudVisitorID and (2) tntID. These identifiers work in tandem with the demdex.net server and the AMCV cookie to help specifically identify users.

94. When a user first visits a site with the Adobe Experience Cloud installed, like when Kaiser Plan Members visit the Site and/or Portal, Adobe checks to see if the AMCV cookie is set. This cookie stores the marketingCloudVisitorID (also known as Experience Cloud ID). According to Adobe, the marketingCloudVisitorID “is a universal and persistent ID that identifies your visitors across all solutions in the Experience Cloud.”¹⁷ In the POST calls referenced above the marketingCloudVisitorID for Plaintiffs are assigned specific numeric values (Redacted for Plaintiff Jane Doe and Redacted for Plaintiff John Doe). This in turn allows for tracking of Kaiser Plan Members across Kaiser Permanente sites and across devices.

95. If the AMCV cookie is not set, the Adobe code places a call to the demdex.net server, which generates a marketingCloudVisitorID and sets the AMCV cookie with that value. It also sets a demdex ID cookie which is persistent.¹⁸ Since the marketingCloudVisitorID is stored in the AMCV cookie, it will remain the same for anyone using the browser for that specific site. When a user visits another site with Adobe Experience Cloud installed, a new marketingCloudVisitorID will be generated, but the demdex ID will remain the same. According to Adobe, “the demdex ID remains the same . . . because it’s contained in a third-party cookie and persists across different domains.”¹⁹ This in turn allows Adobe to track specific devices across sites.

96. According to Adobe the tntID, “can be seen as a device ID.”²⁰ As detailed above, device IDs use the unique setup of a user’s computer and browser to establish a device fingerprint. This fingerprint can track users across various Websites to build a profile based on their Web browsing habits. In the POST calls referenced above the tntID is assigned a specific numeric value

¹⁷ *Adobe Target Delivery API (1.0.0) Terms of Service*, Adobe, <https://developers.adobetarget.com/api/delivery-api/#section/Identifying-Visitors> (last visited June 9, 2023).

¹⁸ *How the Experience Cloud Identity Service requests and sets IDs*, Adobe (Updated Nov. 10, 2022), <https://experienceleague.adobe.com/docs/id-service/using/intro/id-request.html?lang=en>.

¹⁹ *Id.*

²⁰ *Adobe Target Delivery API (1.0.0) Terms of Service*, supra note 17.

(Redacted) for Plaintiff Jane Doe and (Redacted) for Plaintiff John Doe). The tntID is stored in the persistent mbox cookie. Adobe uses the tntID as the main identifier for its Adobe Target solution.²¹ The Adobe Target system is used to personalize a user's experience on a website, like Kaiser Plan Members on the Site and Portal. By default, Adobe Target captures the following data, which in turn allows the website to serve personalized and targeted information to specific users:

Data category	Description
Environment parameters	Information about a user's environment, including operating system, browser, and time of day/day of week.
Geography	Information about a user's geography, obtained via IP lookup.
Mobile device	Information about a user's mobile device.
Target reporting segments	Reporting segments configured in Target reporting.
Session behavior	Information about user behavior, such as number of pages viewed. ²²

97. According to Adobe, the thirdPartyID “is a persistent ID that your business utilizes to identify an end-user regardless of whether they are interacting with your business from web, mobile, or IoT channels. In other words, the thirdPartyId will reference user profile data that can be utilized across channels.”²³ In John Doe's POST call referenced above, the thirdPartyId is assigned a specific numeric value (Redacted). This ID can be used to identify return users once they have logged into the Portal. This in turn allows Adobe's customers to associate the thirdPartyID with a specific individual, the third party here being Kaiser Permanente's patients.

²¹ *Id.*

²² Adapted from: *Data used by Target machine-learning algorithms*, Adobe (Updated Apr. 23, 2023), <https://experienceleague.adobe.com/docs/target/using/activities/automated-personalization/ap-data.html>.

²³ *Adobe Target Delivery API (1.0.0) Terms of Service*, *supra* note 17.

98. The fourth block (grey) includes customerIds that can be, “added and associated with an Experience Cloud Visitor ID.”²⁴ In the case of the POST call above, the additional data includes the fact the user is authenticated (logged in), again signifying that Plaintiff is a Kaiser Plan Member and Kaiser Permanente patient—information which Kaiser Permanente is prohibited from disclosing under HIPAA and other state and federal laws and its express and implied contracts with Kaiser Plan Members.

99. Similar POST calls to kaiser.tt.omtrdc.net were found on all examined pages, including main page (Southern California and Washington), doctor search, retrieving test results, and the bill pay page.

100. After Plaintiff Jane Doe logged into the Portal and accessed test results on May 31, 2023, Adobe intercepted and received information about the fact Plaintiff Jane Doe had lab test results available (see green highlight), which was transmitted to Adobe and stored on Adobe’s kaiser.tt.omtrdc.net server:

```
{
  "requestId": "e89a72b9d34c409ebbec86e8d421e30",
  "context": {
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36",
    "clientHints": {
      "mobile": false,
      "platform": "Windows",
      "browserUAWithMajorVersion": "\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\"",
      "timeOffsetInMinutes": -420,
      "channel": "web",
      "screen": {
        "width": 1366,
        "height": 768,
        "orientation": "landscape",
        "colorDepth": 24,
        "pixelRatio": 1
      },
      "window": {
        "width": 1349,
        "height": 357
      },
      "browser": {
        "host": "wa-member2.kaiserpermanente.org",
        "webGLRenderer": "ANGLE (Intel, Intel(R) HD Graphics Direct3D11 vs_5_0 ps_5_0, D3D11)",
        "address": {
          "url": "https://wa-member2.kaiserpermanente.org/MyChart/inside.asp?mode=labdetail&eorderid=WP-24dwjwXsqOLR9HkFJIJ-2BBnKA9ug2421MnQJWoSc-2Bc79kw-3D-24kgLeo5NOVUqzyhbO5PbT2bSZ1zLoJ7dRShqNeRddSXk-3D",
          "referrerUrl": "https://wa-member2.kaiserpermanente.org/mychart/Clinical/TestResults"
        }
      }
    },
    "id": {
      "tntId": "Redacted",
      "thirdPartyId": "132259249",
      "marketingCloudVisitorId": "Redacted",
      "customerIds": [
        {
          "id": "132259249",
          "integrationCode": "kpaamidepp",
          "authenticatedState": "authenticated",
          "type": "DS"
        },
        {
          "id": "132259249",
          "integrationCode": "kpaamidudr",
          "authenticatedState": "authenticated",
          "type": "DS"
        },
        {
          "id": "132259249",
          "integrationCode": "kpaamid_One-off-datasets",
          "authenticatedState": "authenticated",
          "type": "DS"
        },
        {
          "id": "132259249",
          "integrationCode": "pzn_crm",
          "authenticatedState": "authenticated",
          "type": "DS"
        },
        {
          "id": "132259249",
          "integrationCode": "mbox3rdPartyId",
          "authenticatedState": "authenticated",
          "type": "DS"
        }
      ]
    },
    "experienceCloud": {
      "audienceManager": {
        "locationHint": 9,
        "blob": "6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y",
        "analytics": {
          "logging": "server_side",
          "supplementalDataId": "1926210C0731CEF9-0CC37604F49C1490"
        }
      }
    },
    "execute": {
      "pageLoad": {
        "parameters": {
          "Seg18v": "wa",
          "Seg17v": ""
        }
      }
    }
  }
}
```

²⁴ *Id.*


```

1    wa", "Seg55v": "Logged
2    In", "Seg181v": "", "Seg81v": "", "Seg114vcookie": "mbr", "reEnable": "", "throttle-
3    area": "", "profileParameters": {"region": "", "Seg2": "20"}}, "prefetch": {"views": [{"paramete
4    rs": {"Seg18v": "wa", "Seg17v": "wa", "Seg55v": "Logged
5    In", "Seg181v": "", "Seg81v": "", "Seg114vcookie": "mbr", "reEnable": "", "throttle-
6    area": "", "profileParameters": {"region": "", "Seg2": "20"}}, "telemetry": {"entries": [{"reque
7    stId": 3198432, "timestamp": 1685577421980, "execution": 194.1}, {"execution": 226.7, "parsin
8    g": 0.3, "request": {"tls": 27.7, "timeToFirstByte": 55.3, "download": 6.1, "responseSize": 1005}, "
9    telemetryServerToken": "GRgdNPKF2baxcRHAQqAHq1m+lb9PISy9OC4JmXflkxk=", "mo
10   de": "edge", "features": {"executePageLoad": true, "prefetchViewCount": 1, "decisioningMetho
11   d": "server-
12   side"}, "requestId": "43b0d783fec64ed0a8f15aa346982faa", "timestamp": 1685577421736}}]}
13   }

```

101. After Plaintiff John Doe accessed his medical history from within the Portal, Adobe intercepted and received information about the fact Plaintiff John Doe suffers from headaches (see green highlight), which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

```

14   {"requestId": "8e07062bb9e84eadb2bb393dac657698", "context": {"userAgent": "Mozilla/5.0
15   (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
16   Chrome/113.0.0.0
17   Safari/537.36", "clientHints": {"mobile": false, "platform": "macOS", "browserUAWithMajorV
18   ersion": "\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-
19   A.Brand\";v=\"24\""}, "timeOffsetInMinutes": -
20   420, "channel": "web", "screen": {"width": 1512, "height": 982, "orientation": "landscape", "color
21   Depth": 30, "pixelRatio": 2}, "window": {"width": 1512, "height": 559}, "browser": {"host": "healt
22   hy.kaiserpermanente.org", "webGLRenderer": "ANGLE (Apple, Apple M1 Pro, OpenGL
23   4.1)"}, "address": {"url": "https://healthy.kaiserpermanente.org/southern-
24   california/secure/search-medical-record?uri=search%3ahealth-
25   encyclopedia&type=ICD&queryICD10=R51.9&label=HEADACHE&groupName=Health+
26   summary", "referrerUrl": "https://healthy.kaiserpermanente.org/hconline/ie/inside.asp?lang=
27   english&mode=snapshot"}}, "id": {"tntId": "Redacted", "thi
28   rdPartyId": "Redacted", "marketingCloudVisitorId": "Redacted",
29   "customerIds": [{"id": "Redacted", "integrationCode": "kpaamidepp", "authenticated
30   State": "authenticated", "type": "DS"}, {"id": "Redacted", "integrationCode": "kpaamidudr", "au
31   thenticatedState": "authenticated", "type": "DS"}, {"id": "Redacted", "integrationCode": "kpaa
32   mid_One-off-
33   datasets", "authenticatedState": "authenticated", "type": "DS"}, {"id": "Redacted", "integrationC
34   ode": "pzn_crm", "authenticatedState": "authenticated", "type": "DS"}, {"id": "Redacted", "integ
35   rationCode": "mbox3rdPartyId", "authenticatedState": "authenticated", "type": "DS"}]}, "experi
36   enceCloud": {"audienceManager": {"locationHint": 9, "blob": "6G1ynYcLPuiQxYZrsz_pkqfL
37   G9yMXBpb2zX5dvJdYQJzPXImdj0y"}, "analytics": {"logging": "server_side", "supplementa
38   lDataId": "0E8C61D7B797A752-
39   08C07E6DBCFCB5A"}}, "execute": {"pageLoad": {"parameters": {"Seg18v": "sca", "Seg17
40   v": "sca", "Seg55v": "Logged In", "Seg181v": "", "Seg81v": "kporg:secure:search-medical-
41   record", "Seg114vcookie": "mbr", "reEnable": "", "throttle-
42   area": "", "Seg180v": false, "Seg4": true, "Seg517e": false, "Seg5": false, "Seg6": false, "Seg7": fals
43   e, "Seg8": false, "Seg440e": false, "Seg9": false, "Seg11": false, "Seg20v": 7692006, "Seg114v": "S
44   UBSCRIBER", "Seg13": false, "Seg14": false, "Seg16": false, "Seg19": false, "Seg101v": 27, "Seg
45   516e": false, "Seg126v": false, "modval": 6, "Seg21": 100453, "Seg22": "", "Seg24": "urn:kp:prodi
46   em", "Seg25": false, "entitlement-
47   446": true, "pLoaded": 1, "id": ""}, "profileParameters": {"region": "", "Seg2": "12", "Seg56v": "M
48   BR", "Seg10": "NOT

```

ENROLLED", "Seg20v":7692006, "Seg12": "ACTIVE", "Seg101v":27, "Seg15": "true", "Seg106v": "KFHP_HMO", "Seg6": "false", "pzn_id": "Redacted", "Seg103v": false}}, "prefetch": {"views": [{"parameters": {"Seg18v": "sca", "Seg17v": "sca", "Seg55v": "Logged In", "Seg181v": "", "Seg81v": "kporg:secure:search-medical-record", "Seg114vcookie": "mbr", "reEnable": "", "throttle-area": "", "Seg180v": false, "Seg4": true, "Seg517e": false, "Seg5": false, "Seg6": false, "Seg7": false, "Seg8": false, "Seg440e": false, "Seg9": false, "Seg11": false, "Seg20v": 7692006, "Seg114v": "SUBSCRIBER", "Seg13": false, "Seg14": false, "Seg16": false, "Seg19": false, "Seg101v": 27, "Seg516e": false, "Seg126v": false, "modval": 6, "Seg21": 100453, "Seg22": "", "Seg24": "urn:kp:proditem", "Seg25": false, "entitlement-446": true, "pLoaded": 1, "id": ""}, "profileParameters": {"region": "", "Seg2": "12", "Seg56v": "M BR", "Seg10": "NOT ENROLLED", "Seg20v": 7692006, "Seg12": "ACTIVE", "Seg101v": 27, "Seg15": "true", "Seg106v": "KFHP_HMO", "Seg6": "false", "pzn_id": "Redacted", "Seg103v": false}}, "telemetry": {"entries": [{"requestId": 3198432, "timestamp": 1686077690690, "execution": 12.7}, {"execution": 120.9, "parsing": 0.1, "request": {"tls": 1.8, "timeToFirstByte": 93.3, "download": 0.8, "responseSize": 1658}, "telemetryServerToken": "GRgdNPKF2baxcRHAQqAHqyTPswyQefSCMFGH9GY2aUI=", "mode": "edge", "features": {"executePageLoad": true, "prefetchViewCount": 1, "decisioningMethod": "server-side"}, "requestId": "30377aef3045436aa832ba402fe7c5ca", "timestamp": 1686077690672}]}

102. Similarly, after Plaintiff John Doe accessed his medical history from within the Portal, Adobe intercepted and received information about the fact Plaintiff John Doe suffers from kidney stones (see green highlight), which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

```
{
  "requestId": "c7c2f6533c974a37bf18df244b7860ac",
  "context": {
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36",
    "clientHints": {
      "mobile": false,
      "platform": "macOS",
      "browserUAWithMajorVersion": "\"Google Chrome\\\";v=\\\"113\\\", \\\"Chromium\\\";v=\\\"113\\\", \\\"Not-A.Brand\\\";v=\\\"24\\\"\"",
      "timeOffsetInMinutes": -420,
      "channel": "web",
      "screen": {
        "width": 1512,
        "height": 982,
        "orientation": "landscape",
        "colorDepth": 30,
        "pixelRatio": 2
      },
      "window": {
        "width": 1512,
        "height": 732
      },
      "browser": {
        "host": "healthy.kaiserpermanente.org",
        "webGLRenderer": "ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)",
        "address": {
          "url": "https://healthy.kaiserpermanente.org/southern-california/pages/search?query=kidney+stones&category=global&global-region=sca&language=english&region=sca",
          "referringUrl": "https://healthy.kaiserpermanente.org/southern-california/front-door"
        }
      },
      "id": {
        "tntId": "Redacted",
        "marketingCloudVisitorId": "Redacted",
        "experienceCloud": {
          "audienceManager": {
            "locationHint": 9,
            "blob": "RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"
          },
          "analytics": {
            "logging": "server_side",
            "supplementalDataId": "1385A481D134AE9C-5442EE55E30D9036"
          }
        }
      },
      "execute": {
        "pageLoad": {
          "parameters": {
            "Seg18v": "sca",
            "Seg17v": "",
            "Seg55v": "Logged Out",
            "Seg181v": "",
            "Seg81v": "kporg:pages:search",
            "Seg114vcookie": "",
            "reEnable": "",
            "throttle-area": "",
            "profileParameters": {
              "region": "",
              "Seg2": "12"
            }
          },
          "prefetch": {
            "views": [
              {
                "parameters": {
                  "Seg18v": "sca",
                  "Seg17v": "",
                  "Seg55v": "Logged Out",
                  "Seg181v": "",
                  "Seg81v": "kporg:pages:search",
                  "Seg114vcookie": "",
                  "reEnable": "",
                  "throtle-"
```

tle-
 area":"","profileParameters":{"region":"","Seg2":"12"}}},"telemetry":{"entries":[{"requestId":"3198432","timestamp":1686079858947,"execution":31}, {"execution":347.9,"parsing":0.1,"request":{"tls":1.4,"timeToFirstByte":301.7,"download":0.3,"responseSize":3542},"telemetryServerToken":"13OD8mmKQLOFlv9DVqEli/66cI/n43cYFW7Bbdgc7oQ=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"d1ee96fe7bc44f32a598fa3fa6301fec","timestamp":1686079858912}}]}

103. In another example, when Plaintiff John Doe accessed his medications from within the Portal, Adobe intercepted and received information about the fact Plaintiff John Doe takes a certain medication (see green highlight), which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

```
{
  "requestId": "4b353a7157fe4afb994b10217d877637",
  "context": {
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36",
    "clientHints": {
      "mobile": false,
      "platform": "macOS",
      "browserUAWithMajorVersion": "\"Google Chrome\\\";v=\\\"113\\\", \\\"Chromium\\\";v=\\\"113\\\", \\\"Not-A.Brand\\\";v=\\\"24\\\"\"",
      "timeOffsetInMinutes": -420,
      "channel": "web",
      "screen": {
        "width": 1512,
        "height": 982,
        "orientation": "landscape",
        "colorDepth": 30,
        "pixelRatio": 2
      },
      "window": {
        "width": 1512,
        "height": 559
      },
      "browser": {
        "host": "healthy.kaiserpermanente.org",
        "webGLRenderer": "ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"
      },
      "address": {
        "url": "https://healthy.kaiserpermanente.org/southern-california/health-wellness/drug-encyclopedia/drug.259872"
      },
      "referrerUrl": "https://healthy.kaiserpermanente.org/hconline/inside.asp?lang=english&mode=snapshot"
    },
    "id": {
      "tntId": "Redacted",
      "thirdPartyId": "Redacted",
      "marketingCloudVisitorId": "Redacted",
      "customerIds": [
        {
          "id": "Redacted",
          "integrationCode": "kpaamidepp"
        },
        {
          "id": "Redacted",
          "integrationCode": "kpaamidudr"
        },
        {
          "id": "Redacted",
          "integrationCode": "kpaamid_One-off-datasets"
        },
        {
          "id": "Redacted",
          "integrationCode": "pzn_crm"
        },
        {
          "id": "Redacted",
          "integrationCode": "mbox3rdPartyId"
        }
      ],
      "experienceCloud": {
        "audienceManager": {
          "locationHint": 9,
          "blob": "6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"
        },
        "analytics": {
          "logging": "server_side",
          "supplementalDataId": "1EE577E8629305D2-08A3CF719904939A"
        }
      },
      "execute": {
        "pageLoad": {
          "parameters": {
            "Seg18v": "sca",
            "Seg17v": "sca",
            "Seg55v": "Logged In",
            "Seg181v": "",
            "Seg81v": "kporg:health-wellness:drug-encyclopedia:drug.259872",
            "Seg114vcookie": "mbr",
            "reEnable": "",
            "throttle-area": "",
            "Seg180v": false,
            "Seg4": true,
            "Seg517e": false,
            "Seg5": false,
            "Seg6": false,
            "Seg7": false,
            "Seg8": false,
            "Seg440e": false,
            "Seg9": false,
            "Seg11": false,
            "Seg20v": 7692006,
            "Seg114v": "SUBSCRIBER",
            "Seg13": false,
            "Seg14": false,
            "Seg16": false,
            "Seg19": false,
            "Seg101v": 27,
            "Seg516e": false,
            "Seg126v": false,
            "modval": 6,
            "Seg21": 100453,
            "Seg22": "",
            "Seg24": false,
            "Seg25": false,
            "entitlement-446": "",
            "entity.id": "%monograph_id%",
            "pLoaded": 1,
            "id": ""
          },
          "profileParameters": {
            "region": "",
            "Seg2": "12",
            "Seg56v": "MBR",
            "Seg10": "NOT ENROLLED",
            "Seg20v": 7692006,
            "Seg12": "ACTIVE",
            "Seg101v": 27,
            "Seg15": "true",
            "Seg106v": "KFHP_HMO",
            "Seg6": "false",
            "pzn_id": "Redacted",
            "Seg103v": false
          }
        },
        "prefetch": {
          "views": [
            {
              "parameters": {
                "Seg18v": "sca",
                "Seg17v": "sca",
                "Seg55v": "Logged In",
                "Seg181v": "",
                "Seg81v": "kporg:health-wellness:drug-
```

`encyclopedia:drug.259872", "Seg114vcookie": "mbr", "reEnable": "", "throttle-
 area": "", "Seg180v": false, "Seg4": true, "Seg517e": false, "Seg5": false, "Seg6": false, "Seg7": false,
 "Seg8": false, "Seg440e": false, "Seg9": false, "Seg11": false, "Seg20v": 7692006, "Seg114v": "S
 UBSCRIBER", "Seg13": false, "Seg14": false, "Seg16": false, "Seg19": false, "Seg101v": 27, "Seg
 516e": false, "Seg126v": false, "modval": 6, "Seg21": 100453, "Seg22": "", "Seg24": false, "Seg25"
 : false, "entitlement-
 446": "", "entity.id": "%monograph_id%", "pLoaded": 1, "id": "", "profileParameters": {"region"
 : "", "Seg2": "12", "Seg56v": "MBR", "Seg10": "NOT
 ENROLLED", "Seg20v": 7692006, "Seg12": "ACTIVE", "Seg101v": 27, "Seg15": "true", "Seg10
 6v": "KFHP_HMO", "Seg6": "false", "pzn_id": "Redacted", "Seg103v": false}}}, "telemetry": {
 "entries": [{"requestId": 3198432, "timestamp": 1686077727535, "execution": 13.1}, {"executio
 n": 536, "parsing": 0.1, "request": {"tls": 29.6, "timeToFirstByte": 453.5, "download": 9, "response
 Size": 1652}, "telemetryServerToken": "ytSZo63c32LTWU3OagsNm4f2oPeqNn97fefLHdLz
 nd4=", "mode": "edge", "features": {"executePageLoad": true, "prefetchViewCount": 1, "decisio
 ningMethod": "server-
 side"}, {"requestId": "de495a765e94495db656689de5179016", "timestamp": 1686077727519}]}
 }}`

104. When Plaintiff Jane Doe logged out of the Portal and conducted a search for a doctor
 using the keyword “mental health” on the Site, the POST to kaiser.tt.omtrdc.net revealed the search
 term as shown below (green highlight):

`{
 "requestId": "f42ffe0b90c141e6836a7006c18a6965",
 "context": {
 "userAgent": "Mozilla/5.0
 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/113.0.0.0
 Safari/537.36",
 "clientHints": {
 "mobile": false,
 "platform": "Windows",
 "browserUAWithMajor
 Version": "\"Google Chrome\\;v=\\\"113\\\", \\\"Chromium\\;v=\\\"113\\\", \\\"Not-
 A.Brand\\;v=\\\"24\\\"\"",
 "timeOffsetInMinutes": -
 420,
 "channel": "web",
 "screen": {
 "width": 1366,
 "height": 768,
 "orientation": "landscape",
 "color
 Depth": 24,
 "pixelRatio": 1
 },
 "window": {
 "width": 1349,
 "height": 584
 },
 "browser": {
 "host": "healt
 hy.kaiserpermanente.org",
 "webGLRenderer": "ANGLE (Intel, Intel(R) HD Graphics
 Direct3D11 vs_5_0 ps_5_0,
 D3D11)",
 "address": {
 "url": "https://healthy.kaiserpermanente.org/washington/doctors-
 locations#/facility-
 results?zipcode=98203&keyword=mental%20health",
 "referringUrl": "https://healthy.kaiserp
 ermanente.org/doctors-
 locations",
 "beacon": true
 },
 "id": {
 "tntId": "Redacted",
 "marketingCloudVisitorId": "Redacted",
 "experienceClou
 d": {
 "audienceManager": {
 "locationHint": 9,
 "blob": "RKhpRz8krg2tLO6pguXWp5olkAcUni
 QYPHaMWWgdJ3xzPWQmdj0y"
 },
 "analytics": {
 "logging": "server_side",
 "supplementalDat
 aId": "16848F6EF92A646D-
 091DAB5A2A2A31A4"
 }
 },
 "notifications": [
 {
 "id": "12516194156946319b158793ad9744d1",
 "type": "display",
 "timestamp": 1685579001396,
 "parameters": {
 "Seg18v": "wa",
 "Seg17v": "",
 "Seg55v": "Logged Out",
 "Seg181v": "",
 "Seg81v": "kporg:doctors-
 locations",
 "Seg114vcookie": "",
 "reEnable": "",
 "throttle-
 area": ""
 },
 "profileParameters": {
 "region": "",
 "Seg2": "23"
 },
 "view": {
 "name": "facility-
 results"
 }
 }
],
 "impressionId": "2017e8f257b548dbb2e29e2e51bcd38"
 }
 }
 }
 }
}`

105. Similarly, when Plaintiff John Doe logged out of the Portal and conducted a search
 for a neurologist on the Site, the POST to kaiser.tt.omtrdc.net revealed the search term and Plaintiff's
 zip code as shown below (green highlight):


```
{
  "requestId": "c059ddb0f7ee4602ad5c1cf0e72e6e0f",
  "context": {
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36",
    "clientHints": {
      "mobile": false,
      "platform": "macOS",
      "browserUAWithMajorVersion": "\"Google Chrome\";v=\"113\", \"Chromium\";v=\"113\", \"Not-A.Brand\";v=\"24\"",
      "timeOffsetInMinutes": -420,
      "channel": "web",
      "screen": {
        "width": 1512,
        "height": 982,
        "orientation": "landscape",
        "colorDepth": 30,
        "pixelRatio": 2
      },
      "window": {
        "width": 1512,
        "height": 769
      },
      "browser": {
        "host": "healthy.kaiserpermanente.org",
        "webGLRenderer": "ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)",
        "address": {
          "url": "https://healthy.kaiserpermanente.org/southern-california/doctors-locations#/providers?zipcode=92395&medical_specialty_label=Psychiatry%20%26%20Neurology:%20Neurology,Psychiatry%20%26%20Neurology:%20Psychiatry",
          "referringUrl": "https://healthy.kaiserpermanente.org/southern-california/doctors-locations"
        },
        "id": {
          "tntId": "Redacted",
          "marketingCloudVisitorId": "Redacted",
          "experienceCloud": {
            "audienceManager": {
              "locationHint": 9,
              "blob": "RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"
            },
            "analytics": {
              "logging": "server_side",
              "supplementalDataId": "2B0396D39B44DC65-28244F36559B11C5"
            }
          },
          "execute": {
            "pageLoad": {
              "parameters": {
                "Seg18v": "sca",
                "Seg17v": "sca",
                "Seg55v": "Logged Out",
                "Seg181v": "kporg:doctors-locations",
                "Seg114vcookie": "reEnable",
                "throttle-area": "providerType",
                "keyword": "specialty",
                "specialty": "Psychiatry & Neurology: Neurology, Psychiatry & Neurology: Psychiatry",
                "healthPlan": "profileParameters",
                "region": "Seg2",
                "Seg2": "12"
              },
              "prefetch": {
                "views": {
                  "parameters": {
                    "Seg18v": "sca",
                    "Seg17v": "kporg:doctors-locations",
                    "Seg114vcookie": "reEnable",
                    "throttle-area": "providerType",
                    "keyword": "specialty",
                    "specialty": "Psychiatry & Neurology: Neurology, Psychiatry & Neurology: Psychiatry",
                    "healthPlan": "profileParameters",
                    "region": "Seg2",
                    "Seg2": "12"
                  }
                }
              }
            }
          }
        }
      }
    }
  }
}
```

106. On information and belief, the same type of information tracked, disclosed, and sent to Adobe for Plaintiffs has been tracked, disclosed, and sent to Adobe for other members of the Classes.

3. Kaiser Permanente Allows Twitter, Bing, and Google to Intercept Patients' Communications

107. Kaiser Permanente, on its Home Page, Portal Login Page, and other pages on the Site—including within the Portal—also uses code that sends confidential and protected health information to Twitter, Bing, and Google.

108. Google and Bing are the most widely used search engines, and Twitter is one of the largest social media sites in the world. Generally, Google, Bing, and Twitter do not charge to use their services because they are able to generate billions of dollars in revenue each year by selling targeted advertising.

1 109. For example, if a user tweets about a current event in the news or about their job,
2 Twitter and advertisers can understand a user's political leanings or job type. This information is
3 valuable to Twitter because it helps advertisers understand who Twitter users are so that Twitter can
4 sell advertisements targeting that particular user's Twitter timelines.²⁵

5 110. Twitter also tracks browsing activity outside of Twitter, for both Twitter users and
6 people who have never created an account on the Twitter platform, including browser type, the device
7 and operating system, the mobile carrier, IP address, and browsing activity.²⁶ Twitter can also learn
8 information about websites visited before landing on the referring website and what websites were
9 visited after leaving the site.²⁷

10 111. Google and Bing sell ads based on a user's search. So, a search for a medical condition
11 such as cancer, would show ads for cancer treatment centers.

12 112. Google and Bing are also widely used ad platforms that provide ad remarketing.
13 Remarketing shows ads based on sites a user has previously visited. For example, a user who visits a
14 website with Google or Bing code, and searches on pregnancy related topics, might then see ads for
15 a Google or Bing advertiser's pregnancy related services on other websites.

16 113. A main goal for Google, Bing, and Twitter is to develop a profile of users to better
17 target them with ads. Therefore, all these sites offer free analytics tools. These tools are useful to
18 advertisers as they can show how effective certain ads are. Web analytics tools also provide general
19 information about who is visiting the website and what those users are doing on the Site.

20 114. The Kaiser Permanente Website, including inside the Portal, also tracks views via
21 integration with Doubleclick, which is owned by Google and allows companies pay for clicks and
22 track ad effectiveness.

23 115. Bing, Google, and Twitter send data to their respective servers via HTTP GET request
24 parameters.

25
26 ²⁵ Mehak Siddiqui, *What Does Twitter Know About Me?*, vpnoverview (Sept. 9, 2022),
27 <https://vpnoverview.com/privacy/social-media/what-does-twitter-know-about-me/>.

28 ²⁶ *Id.*

²⁷ *Id.*

116. The HTTP GET method requests data from a server. This request can include additional parameters that are sent as part of the request URL. For example, take the request “www.example.com ?utm_source=google.” In this case, everything after the “?” is used to track where the site visitor came from, in this case showing that the visitor came from Google before accessing the www.example.com.

a) Portal Login

117. On May 31, 2023, when Plaintiff Jane Doe logged into the Portal, Bing sent the following GET request to bat.bing.com (color coded here and described in more detail below):

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=0449eabe-5045-4f9c-8768-afbe69c3f01a&sid=147515f0000b11ee937705de2bc479d9&vid=147628d0000b11eeabace7b017e63252&vids=0&mssclkid=N&uach=pv%3D10.0.0&pi=918639831&lg=en-US&sw=1366&sh=768&sc=24&tl=Sign%20in&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fconsumer-sign-on%23%2Fsignon&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fwashington%2Ffront-door<=22894&mtp=10&evt=pageLoad&sv=1&rn=404848

118. On June 6, 2023, when Plaintiff John Doe logged into the Portal, Bing sent the following GET request to bat.bing.com (color coded here and described in more detail below):

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=a57ffab9-4695-4ca1-967a-8733b98911d6&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&mssclkid=N&pi=918639831&lg=en-US&sw=1512&sh=982&sc=30&tl=My%20Health%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fconsumer-interrupt.html<=1125&evt=pageLoad&sv=1&rn=258023

119. The Bing GET request includes temporary and session IDs (mid, sid, vid)—highlighted in yellow above, an indication that the page loaded (green highlight), the URL of the page (blue highlight), and information about the browser and device (grey highlight). The data sent to Bing indicates the user successfully logged into the Portal.

120. According to Bing documentation, “the cookie in the relevant domain and IP address are always passed with every http request and not just via UET.”²⁸ UET is Universal Event Tagging and it’s the method used by Bing to report advertiser activity on a Website. UET was installed on all pages viewed on the Kaiser Website, including within the Portal.

²⁸ *FAQ: Universal Event Tracking*, Microsoft, <https://help.ads.microsoft.com/apex/index/3/en/53056/> (last visited June 9, 2023).

121. When Plaintiff Jane Doe logged into the Portal, Google also sent multiple GET requests to both googleads.g.doubleclick.net and google.com. These requests are essentially similar in nature. For example, the data sent via GET to Google servers at googleads.g.doubleclick.net is below:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1685576958827&cv=11&fst=1685576958827&bg=ffffff&guid=ON&async=1>m=45be35v0&u w=1366&u h=768&url=https%3A%2F%2Fwamember.kaiserpermanente.org%2Fhome%2F&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2F&label=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=Secure%20Member%20Site%20%7C%20Kaiser%20Permanente%20Washington&auid=2067634156.1685575801&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.127%7CChromium%3B113.0.5672.127%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=Windows&uapv=10.0.0&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

122. When Plaintiff John Doe logged into the Portal, Google also sent multiple GET requests to both googleads.g.doubleclick.net and google.com. These requests are essentially similar in nature. For example, the data sent via GET to Google servers at googleads.g.doubleclick.net is below:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1686076950094&cv=11&fst=1686076950094&bg=ffffff&guid=ON&async=1>m=45be35v0&u w=1512&u h=982&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fmedical-record&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&label=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=Medical%20Record%20%7C%20Kaiser%20Permanente&auid=1088085833.1686076832&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

123. The above GET requests includes the URL of the current site (blue highlight), the event type (highlighted in green)—in this case a conversion, as well as data about the browser and device that allows Google to produce a device fingerprint (highlighted in grey). The data sent to Google indicates the user successfully logged into the Portal.

124. When Plaintiff Jane Doe logged into the Portal, Google used the POST method to transmit the following data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je35v0&_p=1252165919&cid=657412457.1685575799&ul=en-us&sr=1366x768&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.127%7CChromium%3B113.0.5672.127%7CNot-

A.Brand%3B24.0.0.0&uamb=0&uam=&uap=Windows&uapv=10.0.0&uaw=0&ngs=1&_s=1&sid=1685575799&sct=1&seg=1&dl=https%3A%2F%2Fwa-member.kaiserpermanente.org%2Fhome%2F&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2F&dt=Secure%20Member%20Site%20%7C%20Kaiser%20Permanente%20Washington&en=page_view&_ee=1&_et=1

125. When Plaintiff John Doe logged into the Portal, Google used the POST method to transmit the following data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je35v0&p=78753540&cid=1504176517.1686076832&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CCromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&ngs=1&s=1&sid=1686076832&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fconsumer-interrupt.html&dt=My%20Health%20%7C%20Kaiser%20Permanente&en=page_view&_ee=1

126. The POST above includes temporary and session IDs (cid, sid)—highlighted in yellow, an indication that the page loaded (green highlight), the URL of the current page (blue highlight), and information about the browser and device (grey highlight). As discussed above, device data allows Google to establish a device fingerprint to track devices across multiple websites. The data sent to Google indicates the user successfully logged into the Portal.

127. When Plaintiff Jane Doe accessed the Portal, Twitter sent two GET requests—one to analytics.twitter.com and one to t.co. Except for the base domain, both GET requests were the same as follows:

https://analytics.twitter.com/1/i/adset?bci=4&eci=3&event=%7B%7D&event_id=5f8ad0cc-d7e4-4c79-be40-b2476d38e9c6&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=751184a7-0132-46b9-80db-fa67ceecceec&tw_document_href=https%3A%2F%2Fwa-member.kaiserpermanente.org%2Fhome%2F&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

128. When Plaintiff John Doe accessed the Portal, Twitter sent two GET requests—one to analytics.twitter.com and one to t.co. Except for the base domain, both GET requests were the same as follows:

https://t.co/1/i/adset?bci=4&eci=3&event=%7B%7D&event_id=23676916-ed52-496b-be38-e9067f36cf37&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=eb369f6b-bab7-443a-abfd-6a18f78ec1e2&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fso

uthern-california%2Fsecure%2Finner-door&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

129. As reflected above, highlighted in blue, the Twitter GET requests were used to indicate a page view of the Portal—indicating the user successfully logged in.

b) Inside the Portal—Accessing Medical Records

130. On June 6, 2023, when Plaintiff John Doe accessed his medical records from within the Portal, Bing, Google, and Twitter all transmitted the fact that Plaintiff John Doe suffers from headaches and kidney stones in their GET requests back to their respective servers. Google also transmitted information about Plaintiff John Doe’s physician back to its server.

131. For example, Bing’s GET requests from the medical records pages were:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=98019729-0e18-4699-bd10-1af56bb6e602&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&mssclid=N&pi=918639831&lg=en-US&sw=1512&sh=982&sc=30&tl=Search%20medical%20records&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DICD%26queryICD10%3DR51.9%26label%3DHEADACHE%26groupName%3DHealth%2Bsummary&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhonline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot<=1469&evt=pageLoad&sv=1&rn=848129

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=5e099d19-6039-4641-8440-aa961649664c&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&mssclid=N&pi=918639831&lg=en-US&sw=1512&sh=982&sc=30&tl=Search%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dkidney%2Bstones%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Ffront-door<=1013&evt=pageLoad&sv=1&rn=975174

132. The Bing GET request above includes the same temporary and session IDs (mid, sid, vid) as the Portal page (yellow highlight), an indication that the page loaded (green highlight), and information about the browser and device (grey highlight), which identifies the computing device and allows for long term tracking. The GET request also transmitted to Bing, the URL of the page (blue highlight), which in this case also includes the fact that Plaintiff John Doe suffers from headaches (first GET request above) and kidney stones (second GET request above). This data can be used to better target ads.

133. Doubleclick's (and Google.com which was essentially similar) GET requests from the medical records page were:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?r
 andom=1686077690514&cv=11&fst=1686077690514&bg=ffffff&guid=ON&asy
 nc=1>m=45be35v0&u_w=1512&u_h=982&url=https%3A%2F%2Fhealthy.kai
 serpermanente.org%2Fsouthern-california%2Fsecure%2Fmedical-
 record%2Fhealth-
 summary&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-
 california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-
 encyclopedia%26type%3DICD%26queryICD10%3DR51.9%26label%3DHEAD
 ACHE%26groupName%3DHealth%2Bsummary&hn=www.googleadservices.co
 m&frm=0&tiba=Health%20Summary%20%7C%20Medical%20Record%20%7C
 %20Kaiser%20Permanente&auid=1088085833.1686076832&uaa=arm&uab=64
 &uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.567
 2.126%7CNot-
 A.Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event
 %3Dgtag.config&rfmt=3&fmt=4

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?r
 andom=1686079885283&cv=11&fst=1686079885283&bg=ffffff&guid=ON&asy
 nc=1>m=45be35v0&u_w=1512&u_h=982&url=https%3A%2F%2Fhealthy.kai
 serpermanente.org%2Fsouthern-
 california%2Fpages%2Fsearch%3Fquery%3Dkidney%2Bstones%26category%3
 Dglobal%26global-
 region%3Dsca%26language%3Denglish%26region%3Dsca&ref=https%3A%2F
 %2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Ffront-
 door&hn=www.googleadservices.com&frm=0&tiba=Search%20%7C%20Kaiser
 %20Permanente&auid=875947082.1686079450&uaa=arm&uab=64&uafvl=Goo
 gle%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-
 A.Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event
 %3Dgtag.config&rfmt=3&fmt=4

134. The above GET requests includes data about the browser and device (grey highlight) and URL data (blue highlight) reveals Plaintiff John Doe suffers from headaches (first GET data above) and kidney stones (second GET data above). This data can be used to better target ads.

135. While Plaintiff John Doe was accessing the medical records page, Google also used the POST method to transmit the following data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-
 ENXTD8TZ70>m=45je35v0&_p=527624076&cid=1504176517.1686076832
 &ul=en-
 us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.56
 72.126%7CChromium%3B113.0.5672.126%7CNot-
 A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0& e
 u=AEA&ngs=1&_s=2&sid=1686076832&sct=1&seg=1&dl=https%3A%2F%2F
 healthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-
 medical-record%3Furi%3Dsearch%253ahealth-
 encyclopedia%26type%3DICD%26queryICD10%3DR51.9%26label%3DHEAD

ACHE%26groupName%3DHealth%2Bsummary&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhconline%2Fie%2Finside.asp%3Fflang%3Denglish%26mode%3Dsnapshot&dt=Search%20medical%20records&en=scroll&epn.percent_scrolled=90

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je3650&_p=200520362&cid=1743351272.1686079450&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CChromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&ngs=1&sid=1686079449&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dkidney%2Bstones%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Ffront-door&dt=Search%20%7C%20Kaiser%20Permanente&_s=1

136. The POSTs above include a temporary session ID (cid)—highlighted in yellow, and information about the browser and device (grey highlight). The URLs of the current page (blue highlight) reveals Plaintiff John Doe suffers from headaches (first POST above) and kidney stones (second POST above). The data sent to Google can be used to better target ads.

137. On June 7, 2023 when Plaintiff John Doe requested an electronic copy of his medical records Google used the POST method to transmit data to sb-ssl.google.com, including the following which specifically disclosed Plaintiff John Doe's name and other personally identifying information:

https://healthy.kaiserpermanente.org/ie/Documents/Released/Download?releaseId=WP-24F8cOV-2F43chhwz40hINz9AQ-3D-3D-24MVZtUU8nDZTmc44v1yuQuiofNjaDbbZ495l9c4zOCgI-3D&docId=WP-24wUdukuLzxp-2FfzWRYqPN1og-3D-3D-24gBNgJlReE8-2BNQgnAhLwt-2BrLft-2Bk2Dbuv2Y72rrLmVfs-3D&downloadedFileName=HealthSummary_Jun_07_2023.zip&idx=0"

"https://healthy.kaiserpermanente.org/ie/Documents/Released/Download?releaseId=WP-24F8cOV-2F43chhwz40hINz9AQ-3D-3D-24MVZtUU8nDZTmc44v1yuQuiofNjaDbbZ495l9c4zOCgI-3D&docId=WP-24wUdukuLzxp-2FfzWRYqPN1og-3D-3D-24gBNgJlReE8-2BNQgnAhLwt-2BrLft-2Bk2Dbuv2Y72rrLmVfs-3D&downloadedFileName=HealthSummary_Jun_07_2023.zip&idx=0

127.0.0.1"Phttps://healthy.kaiserpermanente.org/ie/Documents/Released?from=DownloadMyRecord"R

Nhttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record_____ "U

Qhttps://healthy.kaiserpermanente.org/southern-california/secure/my-medical-record_____ "†

• https://healthy.kaiserpermanente.org/southern-california/support/medical-

requests.html?kp_shortcut_referrer=kp.org/requestrecords_____ "q

mhttps://healthy.kaiserpermanente.org/support/medical-

requests.html?kp_shortcut_referrer=kp.org/requestrecords_____ "3

/https://www.kaiserpermanente.org/requestrecords_____!"
 https://kp.org/requestrecords_____!"
 ehttps://healthy.kaiserpermanente.org/southern-california/secure/medical-record/download-
 health-record"Nhttps://healthy.kaiserpermanente.org/southern-california/secure/medical-
 record* 0JHealthSummary Jun 07 2023.zipP_____Zen-
 IHE_XDM/Redacted1/STYLE.XSL
 IHE_XDM/Redacted1/DOC0038.XML
 O-1 of 1 - My Health Summary.PDF
 INDEX.HTM "
 IHE_XDM/Redacted1/DOC0024.XML
 IHE_XDM/Redacted1/DOC0001.XML
 IHE_XDM/Redacted1/DOC0005.XML
 IHE_XDM/Redacted1/DOC0006.XML
 IHE_XDM/Redacted1/DOC0007.XML
 IHE_XDM/Redacted1/DOC0008.XML
 ,F2ptç• MGðãö†ÆİëÛ+• Æ“CLμ}S,,Å %ø'8 @Â5(0 8 @ J-Chrome/113.0.5672.126/Mac
 OS XPX`• Ðà ø
 ç”
 "https://healthy.kaiserpermanente.org/ie/Documents/Released/Download?releaseId=WP-
 24F8cOV-2F43chhwz40hINz9AQ-3D-3D-
 24MVZtUU8nDZTmc44v1yuQuiofNjaDbbZ495l9c4zOCgI-3D&docId=WP-
 24wUdukuLzxp-2FfzWRYqPNlog-3D-3D-24gBNgJlReE8-2BNQgnAhLwt-2BrLft-
 2Bk2Dbuv2Y72rrLmVfs-
 3D&downloadedFileName=HealthSummary_Jun_07_2023.zip&idx=0
 127.0.0.1"Phttps://healthy.kaiserpermanente.org/ie/Documents/Released?from=Dow
 nloadMyRecord*ehttps://healthy.kaiserpermanente.org/southern-california/secure/medical-
 record/download-health-record0 9 ã•%øxBP_____X p
 ç• _____
 Phttps://healthy.kaiserpermanente.org/ie/Documents/Released?from=DownloadMyRecord
 127.0.0.1"Ohttps://healthy.kaiserpermanente.org/ie/Documents/DownloadMyRecord
 ?lang=english*ehttps://healthy.kaiserpermanente.org/southern-california/secure/medical-
 record/download-health-record0 9 i•%øxBJehttps://healthy.kaiserpermanente.org/southern-
 california/secure/medical-record/download-health-recordP_____X p
 çS_____
 Ohttps://healthy.kaiserpermanente.org/ie/Documents/DownloadMyRecord?lang=english
 127.0.0.10 9 °•%øxBB
 Jhttps://healthy.kaiserpermanente.org/hconline/ie/inside.asp?lang=english&mode=download
 summaryBQ
 Ohttps://healthy.kaiserpermanente.org/ie/Documents/DownloadMyRecord?lang=englishJeht
 tps://healthy.kaiserpermanente.org/southern-california/secure/medical-record/download-
 health-recordP

138. The above POST data includes the fact that Plaintiff John Doe requested an electronic copy of his medical records on June 7, 2023 (highlighted in green) and Plaintiff John Doe's first name (redacted above).

139. Twitter's (both analytics.twitter.com and t.co) GET request from the medical records page was:

https://t.co/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=305bd815-e13e-4eae-able-

0fd5d4dfea93&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=85138
e85-2f71-4efc-ae39-
6cb490e93e87&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente
.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-
record%3Furi%3Dsearch%253ahealth-
encyclopedia%26type%3DICD%26queryICD10%3DR51.9%26label%3DHEAD
ACHE%26groupName%3DHealth%2Bsummary&tw_iframe_status=0&txn_id=o
2f67&type=javascript&version=2.3.29

https://t.co/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=bdd9fe2d-11a0-
4c14-9ea9-
075f29bd4fe4&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=3e2eb
f5e-3ab3-4c45-8573-
df51ad40350a&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.
org%2Fsouthern-
california%2Fpages%2Fsearch%3Fquery%3Dkidney%2Bstones%26category%3
Dglobal%26global-
region%3Dsca%26language%3Denglish%26region%3Dsca&tw_iframe_status=0
&txn_id=o2f67&type=javascript&version=2.3.29

140. The Twitter GET requests reveal in the current site URL (highlighted in blue) that Plaintiff John Doe suffers from headaches (first GET above) and kidney stones (second GET above). This data can be used to better target ads, in this case showing, for example, headaches so that Plaintiff John Doe could be targeted for such things as pain medication.

141. On information and belief, similar information about other Class Members is also transmitted to Bing, Google, and Twitter when Class Members access their medical records and/or request their medical records on the Portal.

c) Other Activities Within the Portal

142. On June 6, 2023 when Plaintiff John Doe accessed the prescriptions page from within the Portal Bing's GET request was:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=b5c83174-b4ea-4868-b60f-
99002dea9a80&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6
fle2c50f5&vids=0&mssclkid=N&pi=918639831&lg=en-
US&sw=1512&sh=982&sc=30&tl=omeprazole%2020%20mg%20capsule,delayed%20relea
se%20%7C%20Kaiser%20Permanent&p=https%3A%2F%2Fhealthy.kaiserpermanente.org
%2Fsouthern-california%2Fhealth-wellness%2Fdrug-
encyclopedia%2Fdrug.259872&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhco
nline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot<=670&evt=pageL
oad&sv=1&rn=325466

143. The Bing GET request above includes the same temporary and session IDs (mid, sid, vid) as the Portal page (yellow highlight), an indication that the page loaded (green highlight), and information about the browser and device (grey highlight), which identifies the computing device and

allows for long term tracking. The GET request also transmitted to Bing, the fact that John Doe has been prescribed Omeprazole 20mg delayed release (pink highlight). This data can be used to better target ads.

144. Doubleclick and Google (which are essentially the same) GET request from the medications page within the Portal was:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1686077807673&cv=11&fst=1686077807673&bg=ffffff&guid=ON&async=1>m=45be35v0&u_w=1512&u_h=982&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fdrug-encyclopedia%2Fdrug.259872&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhconline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot&hn=www.googleadservices.com&frm=0&tiba=omeprazole%2020%20mg%20capsule%2Cdelayed%20release%20%7C%20Kaiser%20Permanente&auid=1088085833.1686076832&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CCromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dgtag.config&rfmt=3&fmt=4

145. The above GET requests includes data about the browser and device (grey highlight), the current URL (blue), and data (pink) that reveals Plaintiff John Doe was prescribed Omeprazole 20mg delayed release. This data can be used to better target ads.

146. While Plaintiff John Doe was accessing the medications page, Google also used the POST method to transmit the following data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je35v0&_p=2017317913&cid=1504176517.1686076832&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CCromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&ngs=1&_s=1&sid=1686076832&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fdrug-encyclopedia%2Fdrug.259872&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhconline%2Fie%2Finside.asp%3Flang%3Denglish%26mode%3Dsnapshot&dt=omeprazole%2020%20mg%20capsule%2Cdelayed%20release%20%7C%20Kaiser%20Permanente&en=page_view&_ee=1

147. The above POST includes data about the browser and device (grey highlight), the current URL (blue) and data (pink) that reveals Plaintiff John Doe was prescribed Omeprazole 20mg delayed release. This data can be used to better target ads.

148. Twitter's (both analytics.twitter.com and t.co) GET request from the medications page was:

https://t.co/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=b343cdf0-a3db-4b81-b74c-34a88cc9960f&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=8ce3fde0-7770-42d2-a833-f63cc049e2f5&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fdrug-encyclopedia%2Fdrug.259872&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

149. The Twitter GET request includes the current URL (blue) which includes the drug encyclopedia link for the drug 259872 which is Omeprazole 20mg delayed release.

150. When Plaintiff John Doe conducted a physician search from within the Portal the following GET request was sent to www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je3650&p=786057931&cid=1743351272.1686079450&ul=en-us&sr=1512x982&uaa=arm&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.126%7CCromium%3B113.0.5672.126%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&ngs=1&s=2&sid=1686079449&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fphysicians%2Fevan-mosier-9630484&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fdoctors-locations&dt=Evan%20Alan%20Mosier%2C%20MD%20-%20Gastroenterology%20%7C%20Kaiser%20Permanente&en=user_engagement&_et=20792

151. GET request above includes temporary and session IDs (yellow highlight), information about the browser and device (grey highlight), the current URL (blue highlight), and addition data (pink highlight) which reveals Plaintiff John Doe searched for a gastroenterologist. This data can reveal Plaintiff John Doe's medical condition and can be used for better ad targeting. For example, the data can result in third parties serving ads for antacids or other digestive medications.

d) Other Searches on the Site

152. On May 31, 2023 after Plaintiff Jane Doe logged out of the Portal, Plaintiff Jane Doe conducted a search using the search feature found on the upper right of the main page (Washington) of the Site. On the search results page, Bing sent the following GET request:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=fc8ef6c7-b66b-406b-b1e5-506f755f7359&sid=147515f0000b11ee937705de2bc479d9&vid=147628d0000b11eeabace7b017e63252&vids=0&mssclid=N&uach=pv%3D10.0.0&pi=918639831&lg=en-US&sw=1366&sh=768&sc=24&tl=Search%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2F<=8071&mtp=10&evt=pageLoad&sv=1&rn=424250

153. The Bing GET request above includes temporary and session IDs (mid, sid, vid) (yellow highlight), an indication that the page loaded (green highlight), and information about the browser and device (grey highlight). The GET request also transmitted to Bing the URL of the page (blue highlight), which reveals Plaintiff Jane Doe's search on the term "mental health." Notably, although Plaintiff Jane Doe was logged out of the Portal, Bing was still able to connect the fact that Plaintiff Jane Doe had communicated with Kaiser Permanente about mental health because it had created a digital fingerprint. This data can be used to better target ads.

154. Doubleclick's (and Google.com which was essentially similar) GET request from the search results page was:

`https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1685578748182&cv=11&fst=1685578748182&bg=ffffff&guid=ON&async=1>m=45be35v0&u_w=1366&u_h=768&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2F&hn=www.googleadservices.com&frm=0&tiba=Search%20%7C%20Kaiser%20Permanente&auid=1628977230.1685578549&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.127%7CCromium%3B113.0.5672.127%7CNot-A.Brand%3B24.0.0.0&uamb=0&uap=Windows&uapv=10.0.0&uaw=0&data=event%3Dgtag.config&rfmt=3&fmt=4`

155. The above GET request includes data about the browser and device (grey highlight) and the URL of the page (blue highlight) reveals Plaintiff Jane Doe searched on the term "mental health." This data can similarly be used to better target ads.

156. When Plaintiff Jane Doe conducted a search for "mental health" on the Site, Google used the POST method to transmit the following data to Google servers at www.google-analytics.com:

`https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70>m=45je35v0&_p=1051056236&cid=1313346476.1685578546&ul=en-us&sr=1366x768&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.127%7CCromium%3B113.0.5672.127%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=Windows&uapv=10.0.0&uaw=0&ngs=1&_s=1&sid=1685578545&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fhealth-wellness%2Fmental-health%2Fhow-to-get-care&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&dt=How%20to%20get%20mental%20health%20care%20%7C%20Kaiser%20Permanente&en=page_view&_ec=1`

157. The POST above includes temporary and session IDs (tid, cid, sid), highlighted in yellow, and information about the browser and device (grey highlight). The URL of the current page (blue highlight) reveals Plaintiff Jane Doe searched for the term “mental health.” The data sent to Google can be similarly be used to better target ads.

158. Twitter’s (both analytics.twitter.com and t.co) GET request from the search results page was:

https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=40e2b65d-4a2e-4272-a887-d0a74c97457c&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=bea70ac7-252c-4537-9a9d-754bd29d7111&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

159. The Twitter GET request in the current site URL (highlighted in blue) reveals that Plaintiff Jane Doe searched on the term “mental health.” This data can similarly be used to better target ads.

160. Similarly, when Plaintiff John Doe logged out of the Portal and conducted a search for a physician on the Site the following GET request was sent to Bing:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=9f6a61d7-6328-4bd6-b325-0e5914ecbd5d&sid=9e997de0049911ee92ef43fd7e01cd75&vid=9e99a6f0049911ee89feed6f1e2c50f5&vids=0&mssclkid=N&pi=918639831&lg=en-US&sw=1512&sh=982&sc=30&tl=Find%20Doctors%20and%20Locations%20in%20Southern%20California%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fdoctors-locations%23%2Fproviders%3Fzipcode%3D92395%26medical_specialty_label%3DPsychiatry%2520%2526%2520Neurology%3A%2520Neurology%2CPsychiatry%2520%2526%2520Neurology%3A%2520Psychiatry&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fdoctors-locations<=712&evt=pageLoad&sv=1&rn=110568

161. The Bing GET request above includes temporary and session IDs (mid, sid, vid) (yellow highlight), an indication that the page loaded (green highlight), and information about the browser and device (grey highlight). The GET request also transmitted to Bing the URL of the page (blue highlight), which reveals Plaintiff John Doe’s search for a neurologist or psychiatrist in the 92395 zip code.

1 162. On information and belief, the same type of information tracked, disclosed, and sent
2 to Bing, Google, and Twitter for Plaintiffs has been tracked, disclosed, and sent to Bing, Google, and
3 Twitter for other members of the Classes.

4 163. Whenever Kaiser Plan Members use Kaiser Permanente’s website, Kaiser Permanente
5 allows Bing, Google, and Twitter to intercept the contents of their communications—including
6 personal information, identifying information, and sensitive medical information—without their
7 knowledge, consent, or authorization.

8 164. Kaiser Permanente knowingly redirects and discloses Kaiser Plan Members’
9 personally identifiable patient data, including their status as patients and the contents of their
10 communications with Kaiser Permanente to Bing, Google, and Twitter.

11 165. Despite its legal obligations to keep this information and these communications
12 private and confidential, Kaiser Permanente’s use of Bing, Google, and Twitter analytics causes the
13 redirection, interception, and transmission of the precise content of patients’ communication with
14 Kaiser Permanente to Bing, Google, and Twitter.

15 166. Kaiser Permanente’s unauthorized redirection and disclosures to Bing, Google, and
16 Twitter includes information that identifies Plaintiffs and Class Members as patients of Kaiser
17 Permanente, and aids in receiving and recording patient communications pertaining to or about
18 specific medical conditions, health services, and specific doctors.

19 167. Kaiser Permanente’s disclosures to Bing, Google, and Twitter occur because Kaiser
20 Permanente intentionally deploys Bing, Google, and Twitter code on its website, and that code
21 commandeers Kaiser Plan Members’ web-browsers and causes personally identifiable patient data,
22 as well as the contents of communications exchanged between Kaiser Permanente and its patients, to
23 be redirected and sent to Bing, Google, and Twitter.

24 168. As currently deployed, Bing, Google, and Twitter analytics, as employed by Kaiser
25 Permanente, functions as a wiretap, and Bing, Google, and Twitter as third-party wiretappers.

C. Plaintiffs and Class Members Did Not Consent to Kaiser Permanente Disclosure of Their Information and Communications to Third Parties

169. Kaiser Permanente does not ask Kaiser Plan Members who use its Site and Portal, including Plaintiffs and members of the Classes, whether they consent to having the contents of their information and communications with Kaiser Permanente disclosed to the Third Party Wiretappers. Kaiser Plan Members are never actively told that their electronic communications are being wiretapped by Third Party Wiretappers.

170. Kaiser Permanente states in its Privacy Policy, under the heading “Internet Cookies,” that:

We and our service providers *may* place Internet “cookies” or similar technologies (JavaScript, HTML5, ETag) on the computer hard drives of visitors to the Site. Information we obtain helps us to tailor our Site to be more helpful and efficient for our visitors. For example, we are able to see the navigation path taken by users, and that information allows us to understand user success or challenges with the web experience. *The cookie consists of a unique identifier that does not contain information about your health history.* We use two types of cookies, ‘session’ cookies and “persistent” cookies, along with other similar technologies.

Website and mobile application Privacy Statement, Kaiser, <https://healthy.kaiserpermanente.org/privacy> (last visited June 9, 2023) (emphasis added).

171. This does not disclose that Kaiser Permanente sends Plaintiffs and Class Members’ information and communications to the Third Party Wiretappers.

172. First, these “third parties” are not defined in the Website Privacy Policy.

173. Second, disclosing that others *may* monitor certain information is not the same as disclosing that others *do in fact* collect user data in real time.

174. Third, Kaiser Permanente falsely claims that information about Kaiser Plan Members’ health history is not being transmitted.

175. Fourth, alerting users to the possible use of “cookies . . . and other tracking technologies” does not put Kaiser Plan Members on notice of the use of technology like Session Replay, and other technology used by the Third Party Wiretappers, which, unlike first party cookies, (1) communicate information to an external server as a user navigates a website; (2) track users across devices; (3) are not easily disabled by users; and/or (4) essentially creates a recording of all the information that visitors provide or receive from Kaiser Permanente on the Site.

176. Fifth, disclosures to the Third Party Wiretappers are not made only for the purpose of tailoring the Kaiser Permanente website to be more helpful and efficient for Kaiser Plan Members who use the Site and Portal, but is instead used for marketing purposes, including to produce targeted advertising for third parties.

D. Plaintiffs' and Class Members' Health Information Has Actual, Measurable, Monetary Value

177. Kaiser Plan Members' confidential communications and information that Kaiser Permanente allows the Third Party Wiretappers to intercept has monetary value.

178. For example, one recent study asked over a thousand consumers from around the world what price they would demand of third parties for access to their data and found that passwords would fetch \$75.80; health information and medical records themselves average \$59.80; and in third, Social Security numbers were valued at \$55.70.²⁹

179. Some companies, such as Prognos Health, sell what they purport to be de-identified health information from millions of patients.³⁰

180. Due to the difficulty in obtaining health information, illegal markets also exist for such data, with some reporting that health data can be "more expensive than stolen credit card numbers."³¹

E. Kaiser Permanente's Conduct Violates State and Federal Privacy Laws

181. Kaiser Plan Members have a reasonable expectation of privacy in their identifying information, personal and sensitive medical information and communications with Kaiser Permanente and its providers, rooted in state and federal privacy laws as well as Kaiser Permanente's express and implied contracts and disclosures. This includes a reasonable expectation that Kaiser Plan Members' identifying information, personal and sensitive medical information and communications

²⁹ Jonathan Weicher, *Healthcare hacks—how much is your personal information worth?*, Netlib Security, <https://netlibsecurity.com/articles/healthcare-hacks-how-much-is-your-personal-information-worth/> (last visited June 9, 2023).

³⁰ Press Release, *Prognos Health Announces Patent-Pending Technology* (Apr. 6, 2021), <https://prognoshealth.com/about-us/news/press-release/prognos-health-announces-patent-pending-technology>.

³¹ Aarti Shahani, *The Black Market For Stolen Health Care Data*, NPR (Feb. 13, 2015, 4:55 am), <https://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data>.

1 with Kaiser Permanente and its providers will not be disclosed to or tracked by Third Party
2 Wiretappers and will not be disclosed to third parties for marketing purposes.

3 182. Plaintiffs and Class Members reasonably believed their interactions with Kaiser
4 Permanente on the Site and Portal were private and would not be transmitted to third parties, recorded,
5 or monitored for a later playback.

6 183. The data collected by Kaiser Permanente identified specific web pages navigated and
7 content viewed, and thus revealed personalized and sensitive information about Plaintiffs and Class
8 Members, including sensitive personal and medical information.

9 184. Plaintiffs and Class Members did not have a reasonable opportunity to discover
10 Defendants' unlawful and unauthorized connections and conduct because Kaiser Permanente did not
11 disclose its actions nor seek consent from Plaintiffs or Class Members prior to making the
12 transmissions to third parties.

13 185. Privacy polls and studies uniformly show that the overwhelming majority of
14 Americans consider one of the most important privacy rights to be the need for an individual's
15 affirmative consent before a company collects and shares its customers' personal data.

16 186. For example, a study by Pew Research Center indicated that an overwhelming
17 majority of Americans—approximately 79%—are concerned about how data is collected about them
18 by companies.³²

19 187. As Kaiser Plan Members, Plaintiffs and Class Members have a reasonable expectation
20 of privacy that Kaiser Permanente, their health care provider, will not disclose the content of their
21 personal and medical information and confidential communications with Kaiser Permanente and its
22 providers to third parties without their express authorization.

23 188. Plaintiffs and Class Members' reasonable expectation of privacy in their personally
24 identifiable data and communications exchanged with Kaiser Permanente and its providers is derived
25 from several sources, including:

26 ³² Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control*
27 *Over Their Personal Information*, Pew Research Center (Nov. 15, 2019),
28 <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

- a. Kaiser Permanente's status as Kaiser Plan Members' health care provider;
- b. Kaiser Permanente's common law obligation to maintain confidentiality of patient data and communications;
- c. State and federal laws and regulations protecting the confidentiality of medical information;
- d. State and federal laws protecting the confidentiality of communication and computer data;
- e. Defendants' express promises of privacy and confidentiality; and
- f. Defendants' implied promises of privacy and confidentiality.

189. Significantly, patient health care data in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by the HHS.

190. The HIPAA Privacy Rule, located at 45 CFR § 160 and Subparts A and E of § 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."³³

191. The Privacy Rule broadly defines "protected health information" ("PHI") as "individually identifiable health information" ("IIHI") that is "(i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

192. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

³³ *The HIPAA Privacy Rule*, HHS, <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> (last visited June 9, 2023).

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

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

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

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

197. Guidance from HHS confirms that patient status is protected by HIPAA, which provides

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data. . . . ***If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.***³⁴

³⁴ *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5, HHS (Nov. 26, 2012), <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/>

198. HHS' guidance for marketing communications states that health care providers may not provide patient lists for marketing purposes without the consent of every included patient:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. **Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.**³⁵

199. HHS has previously instructed that patient status is protected by the HIPAA Privacy Rule:

- a. "[T]he sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);
- b. "[A] covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);
- c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and
- d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

V. TOLLING

200. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

201. The statutes of limitations applicable to Plaintiffs' and the Classes' claims were tolled by Defendants' conduct and Plaintiffs and Class Members' delayed discovery of their claims.

202. As alleged above, Plaintiffs and members of the Classes did not know and could not have known when they used the Kaiser Permanente Site and/or Portal that Kaiser Permanente was

coveredentities/De-identification/hhs_deid_guidance.pdf. (emphasis added) (last visited June 9, 2023).

³⁵ *Marketing* at 1-2, Office for Civil Rights (Rev. Apr. 3, 2003), <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf>. (emphasis added).

disclosing their information and communications to third parties. Plaintiffs and members of the Classes could not have discovered Kaiser Permanente's unlawful conduct with reasonable diligence.

203. Kaiser Permanente secretly incorporated the Third Party Wiretappers' code into the Site, including the Portal, providing no indication to Kaiser Plan Members and Site users that their communications would be disclosed to these third parties.

204. Kaiser Permanente had exclusive and superior knowledge that the Third Party Wiretappers' code incorporated on its Site would disclose Kaiser Plan Members' protected and private information and confidential communications, yet failed to disclose to Kaiser Plan Members and Site users, including Plaintiffs and members of the Classes, that by interacting with the Kaiser Permanente Site and/or Portal that Plaintiffs and Class Members' patient status, personal information, sensitive health information, and confidential communications would be disclosed to third parties.

205. Plaintiffs and members of the Classes could not with due diligence have discovered the full scope of Kaiser Permanente's conduct because the incorporation of the Third Party Wiretappers' code is highly technical and there were no disclosures or other indication that would inform a reasonable consumer or Site user that Kaiser Permanente was disclosing and allowing the interception of such information to these third parties.

206. The earliest Plaintiffs and Class Members could have known about Defendants' conduct was shortly before the filing of this Complaint.

VI. CLASS ACTION ALLEGATIONS

207. Plaintiffs bring this action pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(2) and/or (b)(3) on behalf of the following Class and Sub-Classes:

Nationwide Class: All Kaiser Plan Members in the United States who used the Kaiser Permanente website.

California Sub-Class: All Kaiser Plan Members who are residents of the State of California and used the Kaiser Permanente website.

Washington Sub-Class: All Kaiser Plan Members who are residents of the State of Washington and used the Kaiser Permanente website.

Nationwide Breach of Contract Sub-Class: All Kaiser Plan Members who used the Portal on the Kaiser Permanente website.

California Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the State of California and used the Portal on the Kaiser Permanente website.

Washington Breach of Contract Sub-Class: All Kaiser Plan Members who are residents of the State of Washington and used the Portal on the Kaiser Permanente website.

208. Excluded from the Class and Sub-Classes are Defendants and their parents, subsidiaries, and corporate affiliates. Plaintiffs reserve the right to revise the definition of the Class and Sub-Classes based upon subsequently discovered information and reserves the right to establish additional Sub-Class where appropriate. The Class and Sub-Classes are collectively referred to herein as the “Class” or “Classes.”

209. The Classes are so numerous that joinder of all members is impracticable. Plaintiffs believe that there are at least tens of thousands of proposed members of the Classes throughout the United States.

210. Common questions of law and fact exist as to all members of the Classes and predominate over any issues solely affecting individual members of the Classes. The common and predominating questions of law and fact include, but are not limited to:

- Whether Defendants’ acts and practices violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*;
- Whether Defendants’ acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;
- Whether Defendants’ acts and practices violated California’s Constitution, Art. 1, § 1;
- Whether Defendants’ acts and practices violated the Washington Privacy Act Rev. Code of Washington § 9.73, *et seq.*;
- Whether Defendants’ acts and practices violated the Washington Health Care Information Act Rev. Code of Washington § 70.02.005, *et seq.*;
- Whether Defendants’ acts and practices violations Plaintiffs and Class Members’ common law privacy rights;
- Whether Defendants breached a express contract;
- Whether Defendants breached an implied contract; and
- Whether damages, restitution, equitable, injunctive, compulsory, or other relief is warranted.

211. Plaintiffs’ claims are typical of the claims of the Classes that Plaintiffs seek to represent. As alleged herein, Plaintiffs and the Classes sustained damages arising out of the same unlawful actions and conduct by Defendants.

212. Plaintiffs are willing and prepared to serve the Classes in a representative capacity with all of the obligations and duties material thereto. Plaintiffs will fairly and adequately protect the

1 interests of the Classes and has no interest adverse to or in conflict with the interests of the other
2 members of the Classes.

3 213. Plaintiffs' interests are co-extensive with and are not antagonistic to those of absent
4 members within the Classes. Plaintiffs will undertake to represent and protect the interests of absent
5 members within the Classes and will vigorously prosecute this action.

6 214. Plaintiffs have engaged the services of the undersigned counsel. Counsel is
7 experienced in complex litigation, will adequately prosecute this action and will assert and protect
8 the rights of, and otherwise represent, Plaintiffs and absent members of the Classes.

9 215. A class action is superior to all other available methods for the fair and efficient
10 adjudication of this controversy. Plaintiffs know of no difficulty to be encountered in the management
11 of this litigation that would preclude its maintenance as a class action.

12 216. Class action status is warranted under Federal Rule of Civil Procedure 23(b)(3)
13 because questions of law or fact common to the members of the Classes predominate over any
14 questions affecting only individual members, and a class action is superior to other available methods
15 for the fair and efficient adjudication of this controversy.

16 217. The Classes may also be certified under Federal Rule of Civil Procedure 23(b)(2)
17 because Defendants have acted on grounds generally applicable to the Classes, thereby making it
18 appropriate to award final injunctive relief or corresponding declaratory relief with respect to the
19 Classes.

20 218. The interest of members within the Classes individually controlling the prosecution of
21 separate actions is theoretical and not practical. The Classes have a high degree of similarity and are
22 cohesive, and Plaintiffs anticipate no difficulty in the management of this matter as a class action.

23 219. The nature of notice to the proposed Classes is contemplated to be by direct mail
24 and/or email upon certification of the Classes or, if such notice is not practicable, by the best notice
25 practicable under the circumstance including, *inter alia*, email, publication in major newspapers,
26 and/or on the internet.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

**Violation of the Electronic Communications Privacy Act, 18 U.S.C §§ 2510, *et seq.*
(On Behalf of the Nationwide Class)**

220. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

221. Plaintiffs bring this claim individually and on behalf of the Nationwide Class.

222. The Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §§ 2510, *et seq.*, prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

223. The ECPA confers a civil cause of action on “any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter.” 18 U.S.C. § 2520(a).

224. The ECPA protects both the sending and receipt of communications.

225. A violation of the ECPA occurs where any person “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication” or “intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication” or “intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication.” 18 U.S.C. §§ 2511(1)(a), (c)-(d).

226. In addition, “a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.” 18 U.S.C. § 2511(3)(a).

227. “Intercept” means “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4).

1 228. “Electronic communication” means “any transfer of signs, signals, writing, images,
2 sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,
3 electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.”
4 18 U.S.C. § 2510(12).

5 229. “Contents” includes “any information concerning the substance, purport, or meaning”
6 of the communication at issue. 18 U.S.C. § 2510(8).

7 230. An “electronic communication service” means “any service which provides to users
8 thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).

9 231. Plaintiffs and Nationwide Class Members’ communications with Kaiser Permanente
10 through the Site, including the Portal, are electronic communications under the ECPA.

11 232. Whenever Plaintiffs and Nationwide Class Members communicated with Kaiser
12 Permanente and/or their health care providers on the Site, Third Party Wiretappers, through the source
13 code Kaiser Permanente embedded and ran on its website, contemporaneously and intentionally
14 intercepted, and endeavored to intercept Plaintiffs and Nationwide Class Members’ electronic
15 communications without authorization or consent.

16 233. Whenever Plaintiffs and Nationwide Class Members communicated with Kaiser
17 Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source
18 code it imbedded and ran on its website, contemporaneously and intentionally disclosed, and
19 endeavored to disclose the contents of Plaintiffs and Nationwide Class Members’ electronic
20 communications to the Third Party Wiretappers, without authorization or consent, and knowing or
21 having reason to know that the electronic communications were obtained in violation of the ECPA.

22 234. Whenever Plaintiffs and Nationwide Class Members communicated with Kaiser
23 Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source
24 code it embedded and ran on the Site, contemporaneously and intentionally used, and endeavored to
25 use and allow the contents of Plaintiffs and Nationwide Class Members’ electronic communications
26 to be disclosed and used for purposes other than providing health care services to Plaintiffs and
27

1 Nationwide Class Members without authorization or consent, and knowing or having reason to know
2 that the electronic communications were obtained in violation of the ECPA.

3 235. Whenever Plaintiffs and Nationwide Class Members communicated with Kaiser
4 Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source
5 code it embedded and ran on the Site, contemporaneously and intentionally redirected the contents
6 of Plaintiffs and Nationwide Class Members' electronic communications while those
7 communications were in transmission, to persons or entities other than an addressee or intended
8 recipient of such communication, namely the Third Party Wiretappers.

9 236. Whenever Plaintiffs and Nationwide Class Members communicated with Kaiser
10 Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source
11 code it embedded and ran on the Site, contemporaneously and intentionally divulged the contents of
12 Plaintiffs and Nationwide Class Members' electronic communications while those communications
13 were in transmission, to persons or entities other than an addressee or intended recipient of such
14 communication, namely the Third Party Wiretappers.

15 237. The Third Party Wiretappers intentionally intercepted and used the contents of
16 Plaintiffs and Nationwide Class Members' electronic communications for the unauthorized purpose
17 of profiting from Plaintiffs and Nationwide Class Members' communications, including by
18 generating advertising revenue.

19 238. Plaintiffs and Nationwide Class Members did not authorize Kaiser Permanente to
20 disclose the content of their communications with Kaiser Permanente to the Third Party Wiretappers.

21 239. Plaintiffs and Nationwide Class Members did not authorize the Defendants'
22 interception, redirection, disclosure, and/or use of their sensitive, private health information and
23 communications in their electronic communications with Kaiser Permanente. The Third Party
24 Wiretappers are not party to these communications.

25 240. Because the interception of Plaintiffs and Nationwide Class Members'
26 communications was without authorization and consent from Plaintiffs and Nationwide Class
27
28

Members, and included confidential information protected under HIPAA, the interception was unlawful, tortious, and/or constituted a criminal act.

241. Defendants' actions were at all relevant times knowing, willful, and intentional.

242. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Nationwide Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the ECPA and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made as a result of the violation, or (b) statutory damages of whichever is the greater of \$100 per day per violation or \$10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

SECOND CLAIM FOR RELIEF
Violation of the California Invasion of Privacy Act
Cal. Penal Code §§ 630, *et seq.* ("CIPA")
(On Behalf of the Nationwide Class, or alternatively, On Behalf of the California Sub-Class)

243. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

244. Plaintiffs bring this claim individually and on behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class.

245. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*, to address "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.* § 630. CIPA is intended "to protect the right of privacy of the people of this state." *Id.*

246. To establish liability under section 631(a), Plaintiffs need only establish that a Defendant, "by means of any machine, instrument, or contrivance, or in any other manner," did any of the following:

[i] [I]ntentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

1 Or

2 [ii] [W]illfully and without the consent of all parties to the communication, or in
3 any unauthorized manner, reads or attempts to read or learn the contents or meaning
4 of any message, report, or communication while the same is in transit or passing
over any wire, line or cable or is being sent from or received at any place within
this state,

5 Or

6 [iii] [U]ses, or attempts to use, in any manner, or for any purpose, or to
communicate in any way, any information so obtained,

7 Or

8 [iv] [A]ids, agrees with, employs, or conspires with any person or persons to
unlawfully do, or permit, or cause to be done any of the acts or things mentioned
above in this section.

9 247. Under § 631, a defendant must show it had the consent of all parties to a
10 communication.

11 248. Kaiser Permanente and the Third Party Wiretappers are each a “person” for the
12 purposes of CIPA.

13 249. Defendants maintain their headquarters in California, where they designed, contrived,
14 agreed, conspired, effectuated, aided, and/or received the interception and use of the contents of
15 Plaintiffs and Class Members’ communications.

16 250. The Third Party Wiretappers’ code, Quantum Metric’s recording code, Plaintiffs and
17 Class Members’ browsers and Plaintiffs and Class Members’ computing and mobile devices are all
18 a “machine, instrument, or contrivance, or . . . other manner” used to engaged in the prohibited
19 conduct at issue here. Cal. Penal Code § 631.

20 251. Kaiser Permanente installed the Third Party Wiretappers’ code to automatically and
21 secretly spy on, and intercept Plaintiffs and Class Members’ communications with Kaiser Permanente
22 through the Kaiser Permanente website in real time.

23 252. At all relevant times, Kaiser Permanente’s disclosure of Plaintiffs and Class Members’
24 internet communications to Third Party Wiretappers was without Plaintiffs and Class Members’
25 authorization or consent.
26
27
28

253. By installing the Third Party Wiretappers' code on its website, Kaiser Permanente intentionally caused Plaintiffs and Class Members' communications to be intercepted, recorded, stored, and transmitted to the Third Party Wiretappers.

254. At all relevant times, the Third Party Wiretappers intentionally tapped or made unauthorized connections with, the lines of internet communication between Plaintiffs and Class Members and Kaiser Permanente's Site without the consent of all parties to the communication.

255. The Third Party Wiretappers willfully read or attempt to read or learn the contents or meaning of Plaintiffs and Class Members' communications to Kaiser Permanente's Site while the communications are in transit or passing over any wire, line, or cable, or were being received at any place within California when it intercepted Plaintiffs and Class Members' communications with Kaiser Permanente's Site in real time.

256. By embedding the Third Party Wiretappers' technology on its website, Kaiser Permanente aided, agreed with, employed, and conspired with Third Party Wiretappers to carry out the wrongful conduct alleged herein in violation of Cal. Penal Code § 631(a)[iv].

257. Plaintiffs and the Class Members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount of damages sustained by Plaintiffs and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

THIRD CLAIM FOR RELIEF
Common Law Invasion of Privacy—Intrusion Upon Seclusion
(On Behalf of the Nationwide Class, or alternatively, On Behalf of the California Sub-Class)

258. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

259. Plaintiffs bring this claim individually and on behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class.

260. Intrusion upon seclusion has occurred when (1) Defendants intruded and/or aided, agreed with, employed, and/or conspired with the Third Party Wiretappers to intrude into a private place, conversation, matter; (2) in a manner was highly offensive to a reasonable person.

1 261. Kaiser Permanente intentionally intruded upon Plaintiffs and Class Members' solitude
2 or seclusion when it disclosed communications it received from Plaintiffs and Class Members, which
3 was intended to stay private, to Third Party Wiretappers.

4 262. Plaintiffs and Class Members did not consent to or authorize, nor were they aware of
5 (1) Kaiser Permanente's disclosure to Third Party Wiretappers of information that it received from
6 Plaintiffs and Class Members through its Site or (2) the Third Party Wiretappers' collection of
7 information concerning Plaintiffs and Class Members' activity on the Kaiser Permanente website at
8 the time that the disclosure occurred. Plaintiffs and Class Members never agreed that Kaiser
9 Permanente could disclose their communications to Third Party Wiretappers, nor did they agree that
10 the Third Party Wiretappers could collect such information.

11 263. Plaintiffs and Class Members had a reasonable expectation of privacy over their
12 communications with Kaiser Permanente, including information obtained from their use of Kaiser
13 Permanente's Site, including the Portal.

14 264. Kaiser Permanente's and the Third Party Wiretappers' intentional intrusion into
15 Plaintiffs and Class Member's communications with Kaiser Permanente, including information
16 obtained from their use of Kaiser Permanente's Site, was highly offensive to a reasonable person in
17 that it violated federal and state criminal and civil laws designed to protect individual privacy.

18 265. The disclosure and collection of communications with Kaiser Permanente, including
19 information obtained from their use of Kaiser Permanente's Site through deceit is highly offensive to
20 a reasonable person. Plaintiffs and Class Members reasonably expected that their communications
21 with Kaiser Permanente, including information obtained from their use of Kaiser Permanente's Site
22 would not be disclosed to third parties.

23 266. Secret disclosure and collection of Plaintiffs and Class Members' communications
24 with Kaiser Permanente, including information of thousands of individuals obtained from their use
25 of Kaiser Permanente's Site is highly offensive to a reasonable person. Privacy polls and studies show
26 that the overwhelming majority of Americans believe one of the most important privacy rights is the
27 need for an individual's affirmative consent before personal information is collected or shared.

1 Permanente's Site, and in providing such information to Kaiser (and receiving information from
2 Kaiser Permanente) without that information being disclosed to Third Party Wiretappers. This
3 legally-protected interest is derived from the common law, the California Constitution's article I,
4 section 1 guarantee of the right to privacy, the ECPA, CIPA, and HIPAA.

5 278. Plaintiffs and Class Members had a reasonable expectation of privacy under the
6 circumstances, including that: (i) the information Kaiser Permanente disclosed to Third Party
7 Wiretappers included information related to patient status, health conditions, identifying information,
8 personal and sensitive information, information related to medical treatment, and confidential
9 communications with Kaiser Permanente and its providers; and (ii) Plaintiffs and Class Members did
10 not consent or otherwise authorize Kaiser Permanente to disclose this private information and these
11 confidential communications to the Third Party Wiretappers.

12 279. Defendants' conduct constituted a serious invasion of privacy that would be highly
13 offensive to a reasonable person in that: (i) the information disclosed by Kaiser Permanente and
14 collected by Third Party Wiretappers was highly sensitive and personal, as protected by the California
15 Constitution; (ii) Kaiser Permanente did not have authorization or consent to disclose this information
16 to any third party, including Third Party Wiretappers, and the Third Party Wiretappers did not have
17 authorization to collect this information; and (iii) the invasion deprived Plaintiffs and Class Members
18 the ability to control the circulation of said information, which is considered a fundamental right to
19 privacy.

20 280. Defendants' invasion violated the privacy rights of thousands of Class Members,
21 including Plaintiffs, without authorization or consent. Their conduct constitutes a severe and
22 egregious breach of social norms.

23 281. As a direct and proximate result of Defendants' actions, Plaintiffs and Class Members
24 have had their privacy invaded and sustained damages and will continue to suffer damages.

25 282. Plaintiffs and Class Members seek appropriate relief for that injury, including but not
26 limited to injunctive relief and damages that will reasonably compensate Plaintiffs and Class
27
28

Members for the harm to their privacy interests as well as a disgorgement of profits earned as a result of their intrusions upon Plaintiffs and Class Members' privacy.

283. Plaintiffs also seek such other relief as the Court may deem just and proper.

FIFTH CLAIM FOR RELIEF

Breach of Express Contract

(On Behalf of the Nationwide Breach of Contract Sub-Class or alternatively, On Behalf of the California Breach of Contract Sub-Class and the Washington Breach of Contract Sub-Class)

284. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

285. Plaintiffs bring this claim individually and on behalf of the Nationwide Breach of Contract Sub-Class, or alternatively, on behalf of the California Breach of Contract Sub-Class and the Washington Breach of Contract Sub-Class.

286. There exists an express contract between Plaintiffs and the Breach of Contract Sub-Class Members on the one side, and Kaiser Permanente on the other, when Plaintiffs and Breach of Contract Sub-Class Members accessed information on the Kaiser Permanente Portal, namely the Terms and Conditions and Privacy Policy for the Kaiser Permanente website (hereinafter referred to as the "express contract" or "Site Terms and Conditions"). A true and correct copy of the Site Terms and Conditions³⁶ currently in effect is attached hereto as Exhibit 1, and a copy of the Privacy Statement, incorporated into the Terms and Conditions, is attached as Exhibit 2.

287. Specifically, at the bottom of the Portal Login Page, Kaiser Permanente agrees, contracts, and warrants that: "By signing in, you agree to our website Terms & Conditions and Privacy Statement." <https://healthy.kaiserpermanente.org/southern-california/register> (last visited June 9, 2023).

288. The Kaiser Permanente Terms & Conditions, available via hyperlink, provides: "Any personal information you submit to the Site (for yourself or someone else) is governed by our Website and KP Mobile Application Privacy Statement." *Terms & Conditions for our Website and Mobile Application*, *supra* note 4.

289. In the Kaiser Permanente Privacy Statement, also available via hyperlink, Kaiser Permanente also agrees, contracts, and warrants that Kaiser Permanente's data collection "is collected

³⁶ The Terms and Conditions are materially identical for all Kaiser Permanente Regions.

1 on an aggregate basis, which means that no personally identifiable information is associated with the
2 data.”

3 290. In the Kaiser Permanente Privacy Statement, Kaiser Permanente states that Kaiser
4 Permanente and its service providers may place “cookies” or similar technologies on the computer
5 hard drives of visitors to the Site, and further agrees, contracts, and warrants that information obtained
6 from cookies is only used to help Kaiser Permanente “tailor our Site to be more helpful and efficient
7 for our visitors.”

8 291. In the Kaiser Permanente Privacy Statement, Kaiser Permanente agrees, contracts, and
9 warrants that “[t]he cookie consists of a unique identifier that does not contain information about
10 your health history.”

11 292. The Kaiser Permanente Privacy Statement also states that Kaiser “may also
12 occasionally use ‘Web beacons’ (also known as ‘clear gifs,’ ‘Web bugs,’ ‘1-pixel gifs,’ etc.)” and
13 Kaiser Permanente also agrees, contracts, and warrants that Kaiser Permanente Kaiser will “not
14 collect any personal health information” through this technology.

15 293. Kaiser Permanente then makes the following promises in the Privacy Statement,
16 which is incorporated as part of the express contract:

- 17 • “Use and disclosure of health information includes using the information to
18 provide treatment to the individual, to make payments for such treatment, and
19 to conduct ongoing quality improvement activities. Our use and disclosure of
20 an individual’s personal information (including health information) is limited
21 as required by state and federal law.”
- 22 • “In addition to web logs, described below, Kaiser Permanente routinely gathers
23 data on Site activity, such as how many people visit the Site, the web pages or
24 mobile screens they visit, where they come from, how long they stay, etc. ***The
25 data is collected on an aggregate basis, which means that no personally
26 identifiable information is associated with the data.*** This data helps us improve
27 our content and overall usage. The information is not shared with other
28 organizations for their independent use.” (emphasis added).

29 294. In addition, Kaiser promises that “we do not collect any personally identifiable
30 information about visitors to the Site. The policies, sources, uses and disclosures of information are
31 outlined in Sections 1 through 20 that follow.”

significant benefit upon Kaiser Permanente—a benefit to which Kaiser Permanente is not entitled—including, but not limited to, increased efficiency, optimized workflow, cost reduction, and receipt of incentive payments from the federal government (HHS) via the Meaningful Use Program. As just one example, Breach of Contract Sub-Class Members use of the patient Portal, to access test results and make appointments, results in Kaiser Permanente being freed up from performing such tasks of scheduling and reporting on test results for patients, thereby cutting down on long phone calls or in-office communications, increasing efficiency and decreasing costs.

303. In fact, according to a blog post on the health policy website, Health Affairs,³⁷ Kaiser Permanente offers “the largest private-sector patient portal in the U.S.,” which “help[s] our health care system improve outcomes and manage resources.” The Portal has led to a “2 to 6.5 percent improvement in Healthcare Effectiveness Data and Information Set (HEDIS) performance measures,” improved patient loyalty by making portal users “2.6 times more likely to remain Kaiser Permanente members,” and shifted patient interactions from in-person to secure messenger.

304. Thus, Kaiser Permanente benefits from Breach of Contract Sub-Class Members’ use of their online Portal by: (1) making their provision of healthcare services more efficient, and (2) reducing the costs associated with managing their members’ medical conditions. Importantly, as an integrated managed care consortium, Kaiser Permanente is both a healthcare provider and insurer—thus, they are in a position to realize any savings generated by reducing patient costs.

Performance

305. Plaintiffs and Breach of Contract Sub-Class Members performed under the express contract.

Kaiser Permanente’s Breach of the Express Contract

306. Kaiser Permanente materially breached its express contract with Plaintiffs and Breach of Contract Sub-Class Members by disclosing to the Third Party Wiretappers, Plaintiffs and Breach of Contract Sub-Class Members’ patient status, personally identifiable data, and confidential

³⁷ Terhilda Garrido, Brian Raymond, & Ben Wheatley, *Lessons From More Than A Decade In Patient Portals*, Health Affairs (Apr. 7, 2016), <https://www.healthaffairs.org/doi/10.1377/forefront.20160407.054362>.

communications with Kaiser Permanente, thereby failing to provide Plaintiffs and Breach of Contract Sub-Class Members with the secure method of communication it agreed to provide.

307. The patient health information Kaiser Permanente used and disclosed to unauthorized third parties includes:

- a. Breach of Contract Sub-Class Members' IP addresses, User-Agent data, persistent cookie identifiers, device identifiers, and/or browser fingerprint information—all of which constitute personally identifiable data both alone and in combination with other data;
- b. the date and time of Breach of Contract Sub-Class Members' registration for the Portal;
- c. the date and time of every Breach of Contract Sub-Class Members' sign-in and logoff of the "secure" the Portal;
- d. the contents of communications Breach of Contract Sub-Class Members' exchange inside the "secure" Portal;
- e. the contents of communications Breach of Contract Sub-Class Members' exchange after they have logged off the Portal;
- f. the contents of communications Breach of Contract Sub-Class Members' exchange with Kaiser Permanente seeking providers who accept specific insurance products while still signed in to the "secure" Portal; and
- g. all other HTTPS communications patients exchange with Kaiser Permanente and its providers on the Site that Kaiser Permanente has permitted the third parties to correlate with the patient's status as a patient, and the particular dates and times for which they access the "secure" Portal.

308. The patient data Kaiser Permanente discloses (Plaintiffs and Breach of Contract Sub-Class Members' patient status, personally identifiable data, and confidential communications with Kaiser Permanente and its providers) is not aggregated as specified in the Privacy Statement.

309. Nevertheless, information that Plaintiffs and Breach of Contract Sub-Class Members reasonably thought was being transmitted "securely" to Kaiser Permanente was being disclosed by Kaiser Permanente to unauthorized third parties as follows:

- a. A Kaiser Plan Member signs in to the "secure" patient Portal;
- b. On sign-in, Kaiser Permanente discloses the fact of the sign in to Adobe, Bing, Google, Quantum Metric, and Twitter;
- c. Once signed-in, if a Kaiser Plan Member clicked to, for example:
- e. view tests, a disclosure of that action was made to Adobe, Bing, Google, Quantum Metric, and Twitter of the specific tests; or,

- f. Find-A-Doctor, or set an appointment, a disclosure of that action was made to Adobe, Bing, Google, Quantum Metric, and Twitter.
- d. The above examples of patient communications about the doctor or the appointment was shared with Adobe, Bing, Google, Quantum Metric, and Twitter while the Kaiser Plan Member was still logged-in to the “secure” patient Portal; and
- e. On logoff, Kaiser Permanente discloses this action to Adobe, Bing, Google, Quantum Metric, and Twitter.

310. Kaiser Permanente has failed to cure these breaches and continues to disclose to Third Party Wiretappers Plaintiffs and Breach of Contract Sub-Class Members’ personally identifiable data and communications with Kaiser Permanente.

Plaintiffs and Breach of Contract Sub-Class Members Were Damaged

311. Defendants’ breach caused Plaintiffs and Breach of Contract Sub-Class Members the following damages, among others:

- a. Nominal damages for each breach of contract by Defendants;
- b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;
- c. Sensitive and confidential information that Plaintiffs and Breach of Contract Sub-Class Members intended to remain private is no longer private;
- d. Defendants eroded the essential confidential nature of the provider-patient relationship;
- e. Defendants took something of value from Plaintiffs and Breach of Contract Sub-Class Members and derived a benefit therefrom without Plaintiffs and Breach of Contract Sub-Class Members’ knowledge or informed consent and without sharing the benefit of such value;
- f. Plaintiffs and Breach of Contract Sub-Class Members did not get the full value of the medical services for which they paid, which included Defendants’ duty to maintain confidentiality;
- g. Defendants’ actions diminished the value of Plaintiffs and Breach of Contract Sub-Class Members’ personal information;
- h. Defendants’ actions violated the property rights that Plaintiffs and Breach of Contract Sub-Class Member enjoy in their private communications; and
- i. Defendants’ actions violated the property rights that Plaintiffs and Breach of Contract Sub-Class Members enjoy in their personally identifiable medical data and communication.

312. Plaintiffs and Breach of Contract Sub-Class Members also seek attorney’s fees and costs on this claim to the extent allowable.

SIXTH CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of the Nationwide Breach of Contract Sub-Class, or Alternatively, On Behalf of
the California Breach of Contract Sub-Class and the Washington Breach of
Contract Sub-Class)

313. Plaintiffs repeat and incorporate all other paragraphs as if fully set forth herein.

314. Plaintiffs bring this claim on behalf of themselves and the Nationwide Breach of Contract Sub-Class, or alternatively on behalf of the California Breach of Contract Sub-Class and the Washington Breach of Contract Sub-Class.

315. An implied contract was created between Kaiser Permanente, on the one side, and Plaintiffs and Breach of Contract Sub-Class Members, on the other hand, whereby Kaiser Permanente offered to provide Plaintiffs and Breach of Contract Sub-Class Members what it represented to be a secure Portal through which Plaintiffs and Breach of Contract Sub-Class Members could confidentially make appointments, review medical history, get test results, communicate with providers, and find doctors, among other things, and Plaintiffs and Breach of Contract Sub-Class Members agreed to use the purportedly secure Portal to make appointments, view medical history, get test results, and find and communicate with doctors, among other things, instead of doing so by other means, such as by phone or in person.

Mutual Assent

316. Such implied contract was created by virtue of the relationship and conduct of the parties, as well as the surrounding circumstances, including, but not limited to:

- a. The confidential nature of the medical-provider/patient relationship between Kaiser Permanente and Plaintiffs and Breach of Contract Sub-Class Members;
- b. Kaiser Permanente's express promises, as noted above, to maintain the privacy and confidentiality of patients' personally identifiable data and communications that Plaintiffs and Breach of Contract Sub-Class Members exchange with Kaiser Permanente at the Site;
- c. Kaiser Permanente's creation of a purportedly secure patient Portal that requires a sign-in with a user name and password, which would lead a reasonable person to believe that their communications with Kaiser Permanente while signed in to the Portal would not be shared outside of Kaiser Permanente; and
- d. Plaintiffs and Breach of Contract Sub-Class Members' use of the purportedly secure Portal to make appointments, get test results, and find doctors, among other things, instead of doing so by other means, such as by phone or in person.

323. The patient health information Kaiser Permanente used and disclosed to unauthorized third parties for marketing includes:

- a. Breach of Contract Sub-Class Members' IP addresses, User-Agent data, persistent cookie identifiers, device identifiers, and/or browser fingerprint information—all of which constitute personally identifiable data both alone and in combination with other data;
- b. the date and time of Breach of Contract Sub-Class Members' registration for the Portal;
- c. the date and time of every Breach of Contract Sub-Class Member's sign-in and logoff of the "secure" Portal;
- d. the contents of communications Breach of Contract Sub-Class Members exchange inside the "secure" Portal;
- e. the contents of communications Breach of Contract Sub-Class Members exchange after they have logged off the Portal;
- f. the contents of communications Breach of Contract Sub-Class Members exchange with Kaiser Permanente seeking providers who accept specific insurance products while still signed in to the "secure" Portal; and
- g. all other HTTPS communications patients exchange with Kaiser Permanente at the Site that Kaiser Permanente has permitted the third parties to correlate with the Breach of Contract Sub-Class Members' status as a patient and the particular dates and times for which they access the "secure" Portal

324. The patient data Kaiser Permanente discloses (Plaintiffs and Breach of Contract Sub-Class Members patient status, personally identifiable data, and confidential communications with Kaiser Permanente and its providers) is not aggregated as specified in the Privacy Statement.

325. Nevertheless, information that Plaintiffs and Breach of Contract Sub-Class Members reasonably thought was being transmitted "securely" to Kaiser Permanente within the patient Portal was being disclosed by Kaiser Permanente to unauthorized third parties as follows:

- a. A patient signs in to the "secure" patient Portal;
- b. On sign-in, Kaiser Permanente discloses the fact of the sign in to Adobe, Bing, Google, Quantum Metric, and Twitter;
- c. Once signed-in, if a patient clicked to, for example:
- d. view tests, a disclosure of that action was made to Adobe, Bing, Google, Quantum Metric, and Twitter of the specific tests; or,
- e. Find-A-Doctor, or set an appointment, a disclosure of that action was made to Adobe, Bing, Google, Quantum Metric, and Twitter.
- f. The above examples of patient communications about the doctor or the appointment

was shared with Adobe, Bing, Google, Quantum Metric, and Twitter while the patient was still logged-in to the “secure” patient Portal; and

- g. On logoff, Kaiser Permanente discloses this action to Adobe, Bing, Google, Quantum Metric, and Twitter.

326. Kaiser Permanente has failed and refused to cure these breaches and continues to disclose to unauthorized third parties, Plaintiffs and Breach of Contract Sub-Class Members’ patient status, personally identifiable data, and communications with Kaiser Permanente and its providers exchanged on the Site, including the Portal.

Plaintiffs and Breach of Contract Sub-Class Members Were Damaged

327. Defendants’ breach caused Plaintiffs and Breach of Contract Sub-Class Members the following damages, among others:

- a. Nominal damages for each breach of contract by Defendants;
- b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;
- c. Sensitive and confidential information that Plaintiffs and Breach of Contract Sub-Class Members intended to remain private is no longer private;
- d. Defendants eroded the essential confidential nature of the provider-patient relationship;
- e. Defendants took something of value from Plaintiffs and Breach of Contract Sub-Class Members and derived benefit therefrom without Plaintiffs and Breach of Contract Sub-Class Members’ knowledge or informed consent and without sharing the benefit of such value;
- f. Plaintiffs and Breach of Contract Sub-Class Members did not get the full value of the medical services for which they paid, which included Defendants’ duty to maintain confidentiality;
- g. Defendants’ actions diminished the value of Plaintiffs and Breach of Contract Sub-Class Members’ personal information;
- h. Defendants’ actions violated the property rights Plaintiffs and Breach of Contract Sub-Class Members enjoy in their private communications; and
- i. Defendants’ actions violated the property rights Plaintiffs and Breach of Contract Sub-Class Members enjoy in their personally identifiable medical data and communication.

328. Plaintiffs and Breach of Contract Sub-Class Members also seek attorney’s fee and costs on this claim to the extent allowable.

SEVENTH CLAIM FOR RELIEF
Violation of the Washington Privacy Act
Washington Revised Code § 9.73, *et seq.* (“WPA”)
(On Behalf of the Washington Sub-Class)

329. Plaintiff Jane Doe (“Plaintiff” for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

330. Plaintiff brings this claim individually and on behalf of the Washington Sub-Class (the “Sub-Class” for purposes of this subsection).

331. Under Sections 9.73.030(1) and 9.73.030(1)(a) of the Washington Privacy Act (“WPA”), it is unlawful “for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, or record any . . . [p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication.”

332. Under Section 9.73.030(1)(a) of the WPA, a defendant must show it had the consent of all parties to a communication.

333. Kaiser Permanente and the Third Party Wiretappers are each a “person” for the purposes of the WPA.

334. Kaiser Permanente treats patients in Washington and provides access to its website and Patient Portal to patients in Washington, where Kaiser Permanente and the Third Party Wiretappers intercepted Plaintiff and Sub-Class Members’ communications.

335. The Third Party Wiretappers’ code, Quantum Metric’s recording code, Plaintiff’s and Sub-Class Members’ browsers and Plaintiff and Sub-Class Members’ computing and mobile devices are all “device[s] electronic or otherwise designed to record and/or transmit said communication” used to engaged in the prohibited conduct at issue here. Wash. Rev. Code § 9.73.030(1)(a).

336. Kaiser Permanente installed the Third Party Wiretappers’ code to automatically and secretly spy on, and intercept Plaintiffs and Sub-Class Members’ communications with Kaiser Permanente through the Kaiser Permanente website in real time.

337. At all relevant times, Kaiser Permanente's disclosure of Plaintiff and Sub-Class Members' internet communications to Third Party Wiretappers was without Plaintiff and Sub-Class Members' authorization or consent.

338. By installing the Third Party Wiretappers' code on its website, Kaiser Permanente intentionally caused Plaintiff and Sub-Class Members' communications to be intercepted, recorded, stored, and transmitted to the Third Party Wiretappers.

339. At all relevant times, the Third Party Wiretappers intentionally tapped or made unauthorized connections with, the lines of internet communication between Plaintiff and Sub-Class Members and Kaiser Permanente's Site without the consent of all parties to the communication.

340. The Third Party Wiretappers willfully read or attempt to read or learn the contents or meaning of Plaintiff and Sub-Class Members' communications to Kaiser Permanente's Site while the communications are in transit or passing over any wire, line, or cable, or were being received at any place within California when it intercepted Plaintiffs and Sub-Class Members' communications with Kaiser Permanente's Site in real time.

341. By embedding the Third Party Wiretappers' technology on its website, Kaiser Permanente aided, agreed with, employed, and conspired with Third Party Wiretappers to carry out the wrongful conduct alleged herein in violation of Rev. Wash Code §§ 9.73.030 and 9.73.060.

342. Plaintiff and the Sub-Class Members seek statutory damages in accordance with Wash. Rev. Code § 9.73.060, which provides for damages sustained by Plaintiff and the Sub-Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

EIGHTH CLAIM FOR RELIEF
Violation of the Washington Health Care Information Act
Washington Revised Code § 70.02.005, *et seq.* ("HCIA")
(On Behalf of the Washington Sub-Class)

343. Plaintiff Jane Doe ("Plaintiff" for purposes of this subsection) repeats and incorporates all other paragraphs as if fully set forth herein.

344. Plaintiff brings this claim individually and on behalf of the Washington Sub-Class (the "Sub-Class" for purposes of this subsection).

1 345. The Washington Health Care Information Act, Washington Revised Code Sections
2 70.2.005, *et seq.*, states that “a health care provider, an individual who assists a health care provider
3 in the delivery of health care, or an agent and employee of a health care provider may not disclose
4 health care information about a patient to any other person without the patient's written
5 authorization.”

6 346. The Act defines “health care information” to mean “any information, whether oral or
7 recorded in any form or medium, that identifies or can readily be associated with the identity of a
8 patient and directly relates to the patient's health care” Wash. Rev. Code § 70.02.010(17).

9 347. Kaiser Permanente is a health care facility as defined by Wash. Rev. Code §
10 70.010(16).

11 348. By deploying code on its website to capture and transmit its patients’ personally
12 identifiable and health information to third parties, Kaiser Permanente discloses Plaintiff and Sub-
13 Class Members’ health care information without their written authorization.

14 349. As a direct and proximate cause of Kaiser Permanente’s actions, Plaintiff and Sub-
15 Class Members were damaged in that:

16 350. Sensitive, confidential, and/or protected information that Plaintiff and Sub-Class
17 Members intended to remain private is no more;

18 351. Kaiser Permanente took something of value from Plaintiffs and Sub-Class Members
19 and derived benefit therefrom without Plaintiff and Sub-Class Members’ knowledge or informed
20 consent and without sharing the benefit of such value;

21 352. Plaintiff and Sub-Class Members did not get the full value of the medical services for
22 which they paid, which included Kaiser Permanente’s duty to maintain confidentiality of patient data
23 and communications; and

24 353. Kaiser Permanente’s actions diminished the value of Plaintiff and Sub-Class
25 Members’ personally identifiable information, patient data and communications.

26 354. Plaintiff and Sub-Class Members seek an order requiring Kaiser Permanente to
27 comply with the Act, actual damages, and attorney’s fees and costs.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Classes, respectfully requests that the Court enter an order:

- A. Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiffs as the representative of the Classes, and appointing Plaintiffs' counsel as the Class Counsel for the Classes;
- B. Declaring that Defendants' conduct, as set forth above, violates the laws cited herein;
- C. Awarding damages, including nominal, actual, statutory, and punitive damages where applicable, to Plaintiffs and the Classes in an amount to be determined at trial;
- D. Awarding Plaintiffs and the Classes their reasonable litigation expenses, costs and attorneys' fees;
- E. Awarding Plaintiffs and the Classes pre- and post-judgment interest, to the extent allowable;
- F. Awarding such other further injunctive and declaratory relief as is necessary to protect the interests of Plaintiffs and the Classes; and
- G. Awarding such other and further relief as the Court deems reasonable and just.

IX. DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs demand a jury trial as to all issues triable by a jury.

DATED: June 9, 2023

Respectfully submitted,

**KESSLER TOPAZ
MELTZER & CHECK, LLP**

/s/ Jennifer L. Joost
Jennifer L. Joost (Bar No. 296164)
jjoost@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Facsimile: (415) 400-3001

-and-

**KESSLER TOPAZ
MELTZER & CHECK, LLP**

Joseph H. Meltzer
jmeltzer@ktmc.com
Melissa L. Yeates
myeates@ktmc.com
Tyler S. Graden

tgraden@ktmc.com
Jordan E. Jacobson
jjacobson@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

-and-

James E. Cecchi
Michael A. Innes
Kevin G. Cooper
**CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.**
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973)-994-1700
Facsimile: (973)-994-1744
jcecchi@carellabyrne.com
minnes@carellabyrne.com
kcooper@carellabyrne.com

-and-

Zachary Jacobs
**CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.**
222 S Riverside Plaza
Chicago, Illinois 06606
zjacobs@carellabyrne.com

Counsel for Plaintiffs and the proposed Classes

EXHIBIT 1

Terms and Conditions for our Website and Mobile Application

Purpose

Kaiser Permanente provides a website and a mobile app:

- "kaiserpermanente.org," or "healthy.kaiserpermanente.org," or "kp.org" (the Website)
- "KP Mobile Application" (the App), for both iPhone and Android

The Website and the App are referred to collectively in these Terms and Conditions as the "Site."

The Site allows users to:

- view health-related information
- communicate with our practitioners and our staff
- arrange for clinical and health plan services
- access additional services
- consent to receive important communications and documents (such as notices, videos and telephony) regarding their health plan coverage electronically through the email address and/or mobile number specified by the user for this purpose

The information provided on the Site is not a substitute for the advice of a personal physician or other qualified health care professional and does not constitute a diagnosis or professional treatment recommendation. Always seek the advice of a physician or other qualified health care professional with any questions regarding medical symptoms or a medical condition. Never disregard professional medical advice or delay in seeking it because of something you have read on the Site.

If you think you or someone you are taking care of has a medical or psychiatric emergency, call 911 or go to the nearest hospital.

Agreement

BY USING THE SITE OR BY CLICKING "I ACCEPT" BELOW, YOU SIGNIFY YOUR AGREEMENT TO THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT USE THE SITE.

Using secure messaging

Kaiser Permanente provides users with a number of interactive online services to help them better communicate with our practitioners and staff. These services may include (but are not limited to):

- secure messaging, including:
 - email the doctor's office
 - ask a pharmacist
 - appointment requests

You agree that you will not upload or transmit any communications or content of any type (including secure messaging) that infringe upon, misappropriate or violate any rights of any party.

Please note: if you register for the Website before your coverage has started, you will have access to only a limited set of functions prior to when your full coverage begins. If you're registered for the Website, but do not have active coverage, you will have access to records of your past care and coverage, if any.

Viewing medical records

Users may use the Site to view certain information displayed from their medical records, including the results of certain laboratory tests. Using the lab test result feature is considered to be a request to receive lab test results online or on a mobile device.

Users may also authorize other users of the Site to view health information displayed through the "Act for a Family Member" feature. If you are authorized to access another user's health information, you agree to protect the confidentiality of this information and comply with state and federal privacy laws that may prohibit the redisclosure of health information without the express written authorization of the person who is the subject of the health information, including but not limited to federal law prohibiting the redisclosure of health information regarding alcohol and drug abuse referral and treatment.

In addition, although the Site displays certain information in medical records, they do not necessarily display all information found in those medical records. If you think that medical record information displayed on the Site is inaccurate, you can request Kaiser Permanente to amend the medical record by mailing a request to the department identified in your regional Notice of Privacy Practices. (A link to the Regional Notice of Privacy Practices is available at the bottom of each page on the Website) To request a complete copy of a

medical record, please contact the department identified in your regional Notice of Privacy Practices responsible for providing records.

Any personal information you submit to the Site (for yourself or someone else) is governed by our Website and KP Mobile Application Privacy Statement. (A link to our Website and KP Mobile Application Privacy Statement is available at the bottom of each page on our Website and on the "Home" screen at the bottom of the KP Mobile Application.) This includes information on your rights to see and receive copies of your own or others' personal health information.

KP Mobile Application: "Jailbreaking" the mobile operating system

The KP Mobile Application is intended for use only on a mobile device that is running an unmodified manufacturer-approved operating system. Using the KP Mobile Application on a device with a modified operating system may undermine security features that are intended to protect health information from unauthorized or unintended disclosure. You may compromise your health information or the health information of anyone for whom you have been given access, if you use the KP Mobile Application on a mobile device that has been modified. Use of the KP Mobile Application on a mobile device with a modified operating system is a material breach of these Terms and Conditions.

Passwords and Biometric Authentication

Kaiser Permanente has several tools that allow you to record and store information. You are responsible for taking all reasonable steps to ensure that no unauthorized person shall have access to your Kaiser Permanente online password or account. It is your sole responsibility to (1) control the disclosure and use of your activation codes, password reset codes and password; (2) authorize, monitor, and control access to and use of your Kaiser Permanente online account and password; and (3) promptly change your password if you feel it has become compromised; and (4) promptly inform the Site manager of any need to deactivate an account entirely.

To change your password, sign on and choose the arrow icon next to your name at the top of the page. Then, select Profile and Preferences. To deactivate your account, you may contact our Site Manager using the link available at the bottom of each Website web page. If you're using a mobile device and would like to change your password or deactivate your account, please go to the Website and follow the above steps.

If you forget your Website password, among the available methods for resetting your password is the option to choose to have a one-time password reset code sent to either the email address you provided to us when you registered for the Website or via SMS/Text on your primary mobile number on file. To protect your privacy, we recommend that you not use an email address or mobile device that you share with anyone else. To update your email address, sign on to the Website and choose the arrow icon next to your name at the top of the page. Then, select Profile and Preferences and follow the instructions provided. To

update your mobile number, sign on to KP Mobile Application and tap Profile icon on top right corner and follow instructions provided.

If you enable biometric authentication (e.g., iOS or iPadOS Face ID, Touch ID or Android Fingerprint) to sign on to the App, it is your responsibility to be aware that all faces or fingerprints set up on your device for such biometric authentication will be linked to your Website account associated with the App. If other people use the biometric authentication method enabled on your device, they may be able to gain access to your Kaiser account via the App and view information you consider to be private. It is your responsibility to understand the risks of biometric authentication enabled on your mobile device.

You can stop using biometric authentication to sign on to the App at any time. You can elect this option by going to the settings in the App and turning off Face ID/Touch ID/Fingerprint.

Breaches of these Terms and Conditions

In consideration of being allowed to use the Site interactive services, you agree that the following actions shall constitute a material breach of these Terms and Conditions:

- signing on as or pretending to be another person (Note: this does not restrict authorized use of the "Act for a Family Member" feature on the Site.)
- using secure messaging for any purpose in violation of local, state, national, international laws or posted Kaiser Permanente policies
- transmitting material that infringes or violates the intellectual property rights of others or the privacy or publicity rights of others
- transmitting material that is unlawful, obscene, defamatory, predatory of minors, threatening, harassing, abusive, slanderous, or hateful to any person (including Kaiser Permanente personnel) or entity as determined by Kaiser Permanente in its sole discretion
- using interactive services in a way that is intended to harm, or a reasonable person would understand would likely result in harm, to the user or others
- collecting information about others, including email addresses
- intentionally distributing viruses or other harmful computer code
- attempting to (1) probe, scan, "hack", or test the vulnerability of the Site or any Kaiser Permanente system or network; or (2) breach any security or authentication measures on the Site or any Kaiser Permanente system connected to either the Site
- using any "deep-link", "page-scrape", "robot", "spider", data mining tools, data gathering and extraction tools, or other automatic device, program, algorithm or methodology, to (1) access, acquire, copy or monitor any portion of the Site, or (2) in any way reproduce or circumvent the navigational structure or presentation of the Site
- "Jailbreaking" the operating system of a mobile device using the App

Kaiser Permanente expressly reserves the right, in its sole discretion, to terminate a user's access to any interactive services and/or to any or all other areas of the Site due to any act that would constitute a violation of these Terms and Conditions. To the extent there is an inconsistency between these Terms and Conditions and the Website and KP Mobile Application Privacy Statement, these Terms and Conditions shall govern.

Kaiser Permanente may offer interactive areas of the Site under license with Third Party software service providers. These Terms and Conditions extend to and apply to your use of our licensors' software. Our licensors are direct third-party beneficiaries of applicable rights under these Terms and Conditions. By using our licensor's software, you agree to be bound directly to our licensors with respect to your compliance with these Terms and Conditions. Kaiser Permanente may directly enforce the licensors' rights under these Terms and Conditions on the licensors' behalf or a licensor may enforce its rights under these Terms and Conditions directly against you or other users who breach these Terms and Conditions.

Health Care Delivery Communications by email

By accepting these Terms and Conditions, you agree to receive care delivery essential communications by email. These communications may include (but are not limited to):

- notification that an important message awaits you on the Site (this may be a message from a doctor, a new lab test result, an appointment confirmation, a response from a pharmacist, etc.)
- Site and/or service updates
- emergency alerts and critical messages (for example, if a snowstorm or wildfire has temporarily closed a medical center)
- general health communications from Kaiser Permanente providers

While you have Kaiser Permanente coverage, you may receive the monthly *Partners in Health* wellness update by email as part of your essential communications and services. In addition, you may periodically receive online invitations to participate in member satisfaction and other types of surveys related to your experiences at Kaiser Permanente. Your participation in such surveys is always optional.

You should take appropriate precautions to protect personal and confidential information, and to use your devices/apps in a secure and responsible manner. We are not responsible for the security of your devices and we expect that you will configure them in a secure and responsible manner.

We will use a secure transmission method to send you communications that include protected health information (as that term is defined under HIPAA) through e-mail, our Website, and/or Mobile App. While such secure transmission methods provide reasonable protections against unauthorized access, no system can perfectly guard against risks of intentional intrusion or inadvertent disclosure of information sent to us. Moreover, when you transmit information via the internet, your information will be transmitted over a medium that is beyond our control, and therefore the security of the transmission may be compromised before it reaches us. Accordingly, we make no guarantee as to confidentiality or security. If you have concerns regarding the electronic transmission of protected health information, you should consider using non-electronic communication methods to receive documents relating to health plan coverage.

All Kaiser Permanente staff and vendors who have access to, or are involved with, the processing of personal information are trained to respect the confidentiality of your personal information.

Communications by Phone or Text

You verify that any phone information provided to KP is true and accurate, and that you are the current subscriber or owner of any telephone number that you provide.

You acknowledge that by voluntarily providing your telephone number(s), you expressly agree to receive prerecorded voice messages and/or autodialed calls, and text messages from us, our agents, affiliates, and independent contractors related to your relationship with KP. You acknowledge that automated calls or text messages may be made to your telephone number(s) even if your telephone number(s) is registered on any state or federal Do Not Call list. You agree to receive automated calls and text messages from KP, our agents, affiliates, and independent contractors even if you cancel your account or terminate your relationship with us, except if you opt-out (see below).

The text message communications that you may receive from KP may include (but are not limited to):

- A one-time, multifactor authentication (MFA) passcode sent to you after you have opted-in to receiving such a code to authenticate your logging onto the Site
- General health communications from Kaiser Permanente providers including but not limited to notifications regarding upcoming or scheduled appointments, checkups and exams, hospital pre-registration instructions, pre-operative instructions, lab results, post-discharge follow-up, prescription notifications or reminders, or home healthcare instructions
- General health communications relating to your account, registration, changes and updates, service outages, reminders, billing notifications, payment notices, new services available to members, or any transaction with KP
- Marketing and promotional communications

At any time, and even if you have expressly given us permission to send voice/text messages to you, you may communicate your desire not to receive additional voice/text messages by following the stop or opt-out instructions in the voice or text message, by adjusting your preferences on the Website (for only certain categories of communications), or by contacting Member Services.

You acknowledge that neither Kaiser Permanente nor Carriers are liable for delayed or undelivered messages.

As always, message and data rates may apply for any messages sent to you from us and to us from you. If you have any questions about your text plan or data plan, it is best to contact your wireless provider.

You acknowledge that you are aware text messages are not fully secure and could be intercepted by a third party and acknowledge if you share your mobile device with others, they may be able to view text messages sent by Kaiser Permanente. It is your responsibility to understand the risks of receiving text messages on your mobile device. To update your mobile phone number, sign on to the Website and choose the arrow icon next to your name at the top of the page. Then, select Profile and Preferences, and choose "Edit" under "Mobile numbers".

Use by children

We do not knowingly allow minors under the age of 13 to create accounts that allow access to the secured features of the Site.

Access, correction, and data integrity

Although we attempt to maintain the integrity and accuracy of the information on the Site, we make no guarantees as to its correctness, completeness, or accuracy. The Site may contain typographical errors, inaccuracies, or other errors or omissions. Also, unauthorized additions, deletions, or alterations could be made to the Site by third parties without our knowledge. If you believe that information found on the Site is inaccurate or unauthorized, please inform us by contacting our Site Manager. (On the Website, you may Contact our Site Manager using the link available at the bottom of each web page.)

Revisions, changes, and updates

We may revise the information on the Site or otherwise change or update the Site, including these Terms and Conditions, without notice to you. Kaiser Permanente may also make improvements and/or changes in products and/or services described on the Site or add new features at any time without notice. We encourage you to periodically read these Terms and Conditions to see if there have been any changes to our policies that may affect you. Your continued use of the Site will signify your continued agreement to these Terms and Conditions as they may be revised.

Links to Third Party Websites

The Site provides links to other websites that are not owned or controlled by Kaiser Permanente ("Third Party Websites"). We provide links to Third Party Websites as follows.

- Kaiser Permanente provides links to Third Party Websites to connect you easily to additional sources of health information or third party services that may be of interest to you. We may not have any business relationship with the party that controls this type of Third Party Website and a link to such a site is offered only as a convenience to you.
- Kaiser Permanente also provides links to Third Party Websites managed by vendors that we have made arrangements with to offer you services to help you manage your

health or to take and fulfill orders when you purchase items or materials from us. These Third Party Websites may be co-branded, meaning that they display the Kaiser Permanente logo and the logo of the Third Party vendor but they are owned and controlled by the Third Party.

In each such instance, where practicable, we will let you know when you are leaving the Site and linking to a Third Party Website. We may use an icon that we identify with an appropriate legend to let you know when you are leaving the Website.

Kaiser Permanente may not be responsible for the content, security or the privacy practices of Third Party Websites. Please review the privacy statement and any terms of use of each Third Party Website you visit, if applicable. Unless we specifically advise you otherwise, links to Third Party Websites do not constitute or imply endorsement by Kaiser Permanente of those sites, the information they contain or any products or services they describe. Kaiser Permanente does not receive payment or other remuneration in exchange for you linking to or using any Third Party Website.

Deletion (Deactivation) of Your Online Account (App only)

If you request that we delete (deactivate) your online account, we will block access to your online account, but we will not delete any data or other information of the Kaiser Permanente applications or websites associated with that online account. You will not be able to use any Kaiser Permanente mobile applications or websites that use the same user ID and password associated with the online account. If you wish to reactivate your online account to regain access to such Kaiser Permanente mobile applications or websites, please call Member Services. With a deleted (deactivated) online account you'll only be able to receive copies of your medical records by calling Member Services for the contact information of your local medical record office.

This section pertains to the App only.

Consent to Electronic (Paperless) Health Plan Coverage Communications via Website and App

By accepting the terms and conditions and agreeing to this consent to receive communications (all available ones or certain chosen ones) electronically, you consent (agree) to receive essential health plan coverage communications via the Website and/or Mobile App. These communications may include (but are not limited to):

- Coverage and Benefits: Communications and documents pertaining to your coverage and benefits (including cost sharing) for your health plan. Types of documents and communications may include, but are not limited to, Evidence of Coverage, Explanation of Benefits (EOB), Preauthorization and/or Precertification Notices and Preservice letters, Annual Membership Information, Annual Plan Information, and IRS Form 1095-B.

- Billing: Communications and documents related to billing for your Kaiser Permanente Plan may include but are not limited to: Medical Bills, Membership Premium Payment Letters (including delinquency notices), and Premium Bills.
- Cost Estimates: Communications and documents as required of health plan issuers and related to cost estimates for covered services.
- Other types of communication: Other types of communications may include but are not limited to: Communications about your health savings account (HSA) or wellness program awards (if applicable to you), member satisfaction and other surveys (participation is optional), quality information, and other notices that may be required by law.

For a full list of the health plan coverage documents and communications in each category that may be sent electronically, please visit [KP.org/paperless](https://kp.org/paperless).

NOTE: Not all health plan coverage documents and/or communications may be available in your region, for your plan, and/or via the Mobile App. As additional health plan coverage communications and documents are added to those already available electronically, Kaiser Permanente will notify you. You may be asked to consent again to the receipt of documents electronically.

Electronic Delivery of Health Plan Coverage Communications

You have the option to choose which health plan coverage communications and/or documents you receive electronically. You may always change your mind and receive any of your health plan coverage communications or documents in paper copy. To get a copy of a specific health care delivery or health plan coverage communication in paper, log on to your [KP.org](https://kp.org) account and navigate to “My Documents”, click on the specific document you’d like to view and simply save and print the document.

A. Electronic Delivery Method

If you consent to the receipt of communications and documents relating to health plan coverage by electronic delivery, they will be made available electronically through the Website. [and/or Mobile App] All communications that we provide to you in electronic form, will be provided either (1) via email; (2) via the Website as described in an email notice we send to you at the time the information is available; (3) to the extent permissible by law, by access to a Third-Party Website as described in advance for such purpose in an email notice we send to you at the time the information is available; or (4) by an email requesting that you access or download a PDF file from the Website containing the document.

Note: You will have the opportunity to print or save this information about electronic delivery and keep it for your records. By consenting to electronic delivery, you also agree to print out or download all documents we provide to you electronically and keep copies for your records

B. Notification that you have a New Communication

When a new document or communication is delivered electronically through the Website, you will be notified by email to the primary email address found in your Website profile. If Kaiser Permanente receives a notification of delivery failure (i.e. a “bounce message”) that indicates that the primary email address which we have on file for you is no longer valid, we will suspend electronic delivery of all documents and communications and either notify you again using another method (such as text) or return to paper delivery of your documents and communications. We will then mail your communications and/or documents to the last known mailing address on file.

C. Hardware and Software Requirements

In order to access and retain your electronic documents, you will need the following computer hardware and software:

- A computer with an internet connection
- A current web browser that includes 128-bit encryption (e.g., Microsoft Edge , Firefox version 71 or later, Chrome version 49 or later, or Safari version 11 or later) with cookies enabled
- Current Adobe Acrobat Reader version to open documents in PDF format
- A valid email address (your primary email address in your Website profile)
- Sufficient storage space to save past documents or an installed printer to print them

By giving your consent at this time, you agree that you have access to the necessary hardware and software as listed above, and are able to receive, open, and print or download a copy of any document for your records.

We will notify you if there are any material changes to the hardware or software needed to receive electronic documents from Kaiser Permanente at least 30 days in advance of the date any such changes are made. At that time, we will also provide instructions on how to withdraw, change, or renew your consent for electronic delivery of your documents.

D. Updating your Contact Information

It is your responsibility to keep your primary email address up to date so that Kaiser Permanente can communicate with you electronically.

You understand and agree that if Kaiser Permanente sends you an email notification that a communication and/or document was sent and/or an electronic document has been posted, and we do not receive a notification of delivery failure (i.e. a “bounce message”), Kaiser Permanente will be deemed to have provided the communication to and/or document you. This could occur if, for example, you do not receive it because your primary email address on file is blocked by your service provider, or you are otherwise unable to receive electronic communications.

Please note that if you use a spam filter that blocks or re-routes emails from senders not listed in your email address book, you must add the Kaiser Permanente email address to

your email address book so that you will be able to receive the communications we send to you (please consult the instructions of your spam filter for specific directions on how to do this).

You can update your primary email address or mailing address at any time through your Website profile. To change your primary email address and/or mailing address, navigate to the Personal Info section of the Profiles and Preferences page on KP.org website. To update contact information on the KP Mobile Application, click on the profiles and settings icon in the upper right-hand corner and select "Contact Information" from the drop-down menu and follow the instructions.

E. How to Withdraw your Consent

Your consent will remain in effect until your Kaiser Permanente health plan coverage is terminated or you explicitly withdraw your consent by changing your delivery preferences through your Website profile. You may contact the Kaiser Permanente Member Services Call Center by phone and ask a customer service representative to assist you.

When your Kaiser Permanente health plan coverage is terminated, your document(s) will be sent to you by U.S. mail at your last known mailing address on file.

F. Requesting paper copies of electronic communications and documents

If, after you consent to receive your documents electronically, you would like to receive a paper copy of a document we previously sent you, you may request a paper copy within one year of the date we provided the document to you by contacting the Kaiser Permanente Member Services Call Center.

Disclaimer and Limitation of liability

Disclaimer of Warranties

THE SITE, AND ANY CONTENT, INFORMATION, SERVICES OR PRODUCTS OBTAINED THROUGH THE SITE IS PROVIDED "AS IS," WITH ALL FAULTS, WITH NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON INFRINGEMENT. YOUR USE OF THE SITE IS VOLUNTARY, AND AT YOUR OWN RISK. ANY REFERENCES TO SPECIFIC PRODUCTS OR SERVICES ON THE SITE DOES NOT CONSTITUTE OR IMPLY A RECOMMENDATION OR ENDORSEMENT OF SUCH PRODUCTS OR SERVICES BY KAISER PERMANENTE UNLESS SPECIFICALLY STATED OTHERWISE.

Limitation of liability

KAISER PERMANENTE AND ITS AFFILIATES, SUPPLIERS, LICENSORS AND OTHER THIRD PARTIES MENTIONED OR LINKED TO ON THE SITE ARE NEITHER RESPONSIBLE NOR LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE, OR OTHER DAMAGES (INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM LOST PROFITS, LOST DATA, OR BUSINESS INTERRUPTION) ARISING OUT OF OR RELATING IN ANY WAY TO THE SITE, AND ANY CONTENT, INFORMATION, SERVICES OR PRODUCTS OBTAINED THROUGH THE SITE, ANY APP TO WHICH YOU PERMIT KAISER PERMANENTE TO RELEASE DATA (AND INCLUDING, WITHOUT LIMITATION, THE APP'S USE OF ANY DATA YOU MAKE AVAILABLE TO THE APP), AND/OR ANY THIRD PARTY WEBSITE, OR YOUR USE OF ANY OF THE FOREGOING, WHETHER BASED ON WARRANTY, CONTRACT, TORT, OR ANY OTHER LEGAL THEORY AND WHETHER OR NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT AS DESCRIBED IN THE FOLLOWING PARAGRAPH, YOUR SOLE REMEDY FOR DISSATISFACTION WITH THE SITE, SITE-RELATED SERVICES, APPS, AND/OR THIRD PARTY WEBSITES IS TO STOP USING THE SITE, APPS, AND/OR THOSE SERVICES.

APPLICABLE LAWS MAY NOT ALLOW SUCH DISCLAIMER OF WARRANTIES, LIMITATIONS OF LIABILITY, OR THE EXCLUSIONS FROM SUCH LIABILITY, AND YOU MAY BE ENTITLED TO SEEK OTHER REMEDIES UNDER YOUR EVIDENCE OF COVERAGE OR OTHER AGREEMENT WITH KAISER PERMANENTE. IN SUCH CASE, THE ABOVE DISCLAIMERS, LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Choice of law

THESE TERMS AND CONDITIONS ARE GOVERNED BY CALIFORNIA LAW WITHOUT REGARD TO ITS PRINCIPLES OF CONFLICTS OF LAW. IF ANY VERSION OF THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (UCITA) IS ENACTED AS PART OF THE LAW OF CALIFORNIA, THAT STATUTE SHALL NOT GOVERN ANY ASPECT OF THESE TERMS AND CONDITIONS.


Copyrights

Except as otherwise indicated, the Site and all content on the Site, including text, graphics, logos, button icons, photos, images, forms, audio, video, questionnaires, and software, is the property of Kaiser Permanente or its licensors and is protected by United States and international copyright laws. Kaiser Permanente allows you to view or download a single copy of the material on the Site solely for your personal, noncommercial use.

The compilation of all content on the Site is the exclusive property of Kaiser Permanente or, as applicable, its licensors, and is protected by United States and international copyright laws. Unless specifically authorized in writing by Kaiser Permanente, any use of these materials, or of any materials contributed to the Site by entities other than Kaiser Permanente, on any other website or networked computer environment for any purpose is prohibited.

Any rights not expressly granted by these Terms and Conditions or any applicable end-user license agreements are reserved by Kaiser Permanente. Content and features are subject to change or termination without notice in the editorial discretion of Kaiser Permanente.

The Digital Millennium Copyright Act of 1998 (the "DMCA") provides recourse for copyright owners who believe that material appearing on the Internet infringes their rights under U.S. copyright law. If you believe in good faith that materials appearing on the Site infringe your copyright, you (or your agent) may send us a notice requesting that the material be removed, or access to it blocked.

In addition, if you believe in good faith that a notice of copyright infringement has been wrongly filed against you, the DMCA permits you to send us a counter-notice. Notices and counter-notices must meet statutory requirements imposed by the DMCA. One place to find more information is the U.S. Copyright Office website, currently located at <https://www.copyright.gov> .

In accordance with the DMCA, Kaiser Permanente has designated an agent to receive notification of alleged copyright infringement in accordance with the DMCA. Any written Notification of Claimed Infringement should comply with Title 17, United States Code, Section 512(c)(3)(A) and should be provided in writing to our designated agent as follows:

Agent: kp.org Copyright Compliance Department
Address: Kaiser Permanente, KP Digital, 4460 Hacienda Drive, Building A, 3rd floor,
Pleasanton, CA 94588
Fax: 1-925-737-2276
Phone: 1-925-598-2799
Email: ISG.QA-Compliance@kp.org

(This telephone number is for copyright-related complaints only. No solicitations. For member and website services, call 800-556-7677.)

Please note: If you materially misrepresent that online material, product, or activity is infringing your copyrights, you may be liable for damages (including court costs and attorneys' fees) and could be subject to criminal prosecution for perjury. We suggest that you consult your legal advisor before filing a notice or counter-notice.

Trademarks and service marks

"Kaiser Permanente" and the Kaiser Permanente logo are registered service marks of Kaiser Foundation Health Plan, Inc. Other proprietary marks of Kaiser Permanente or third parties may be designated as such from time to time on the Site through use of the TM, SM, or ® symbols. Users of the Site are not authorized to make any use of the Kaiser Permanente marks or the proprietary marks of third parties, including but not limited to, as metatags or in any other fashion that may create a false or misleading impression of affiliation or sponsorship with or by Kaiser Permanente or the applicable third party.

Copyright © 1995 to 2022 Kaiser Permanente. All rights reserved for all countries.

Last updated: June 2022

Version 1.82

EXHIBIT 2

Website and mobile application Privacy Statement

Introduction

Kaiser Permanente provides a website and a mobile app:

- "kaiserpermanente.org," or "healthy.kaiserpermanente.org," or "kp.org" (the Website)
- "KP Mobile Application" (the App), for both iPhone and Android

The Website and the App are referred to collectively in this Privacy Statement as the "Site."

The Site allows our members and other users to view health-related information, communicate with our practitioners and staff, arrange for clinical and health plan services, and access additional services.

This Privacy Statement applies to the Site, which is owned and operated by Kaiser Foundation Health Plan, Inc. ("Kaiser Permanente", "KP"). This Privacy Statement describes how Kaiser Permanente collects and uses the personal information you provide on, and other information that is collected from your use of the Site. It also describes the choices available to you regarding our use of your personal information and how you can access and update this information.

Personal information means information that is individually identifiable. Information that has been de-identified by Kaiser Permanente or others is no longer personal information and is not covered by the terms of this Privacy Statement.

All of your protected health information maintained by Kaiser Permanente, including information you provide on the Site, is also subject to the Notices of Privacy Practices issued by KP under the Health Insurance Portability and Accountability Act ("HIPAA"). The Notices

of Privacy Practices may contain additional provisions relating to the use and disclosure of your information that go beyond the terms of this Privacy Statement.

Kaiser Permanente is committed to protecting the privacy of the users of the Site. We will use and disclose your personal information as stated in this Privacy Statement.

Site Privacy Statement

Use and disclosure of health information includes using the information to provide treatment to the individual, to make payments for such treatment, and to conduct ongoing quality improvement activities. Our use and disclosure of an individual's personal information (including health information) is limited as required by state and federal law. We do not sell or rent personal information about visitors to the Site.

Security

The Site has security measures in place that are intended to help protect against the loss, misuse, unauthorized access or alteration of information under our control both during transmission and once the information is received. These measures include encryption of data using the Secure Socket Layer (SSL) system, and using a secured messaging service when we send your personal information electronically to the Site. Despite these measures, the confidentiality of any communication or material transmitted to or from us via the Site by Internet, text message or email cannot be guaranteed. At your discretion, you may contact us at the mailing address or telephone number listed in the "Questions, complaints, and contacts" section at the end of this Privacy Statement.

Revisions to the Privacy Statement

We may revise this Privacy Statement from time to time as we add new features or modify the way in which we manage information, or as laws change that may affect our services. If we make material changes to our Privacy Statement, we will post notice of this on our Site prior to the changes becoming effective. Any revised Privacy Statement will apply both to information we already have about you at the time of the change, and any personal information created or received after the change takes effect. We include a version number on this Privacy Statement consisting of the date (year, month, and day) it was last revised. We encourage you to periodically reread this Privacy Statement, to see if there have been any changes to our policies that may affect you.

Site visitor data

In addition to web logs, described below, Kaiser Permanente routinely gathers data on Site activity, such as how many people visit the Site, the web pages or mobile screens they visit, where they come from, how long they stay, etc. The data is collected on an aggregate basis, which means that no personally identifiable information is associated with the data. This

data helps us improve our content and overall usage. The information is not shared with other organizations for their independent use.

The Site does not honor a browser's signal or header request not to track the user's activity.

Data caching by mobile applications

In order to ensure a good user experience, certain data may be temporarily or permanently cached by the Mobile Applications on users' mobile devices. Any data that is personally identifiable will be encrypted and will not be viewable by anyone without access to the user's User ID and Password.

Collecting and using and disclosing personal information

Except as disclosed in this Privacy Statement, we do not collect any personally identifiable information about visitors to the Site. The policies, sources, uses and disclosures of information are outlined in Sections 1 through 20 that follow:

1. Information Collection Use

We collect the following personal information from you:

- contact information such as name, email address, mailing address, and phone number
- age or date of birth
- unique identifiers such as username, account number, and password
- preferences information such as preferred first name and the types of emails you'd like to receive from us
- health or medical information (such as health symptoms, health conditions and medications)
- debit and credit card information
- medical record number or health record number if you apply for Kaiser Permanente coverage online, personal health and demographic information about you and those dependents for whom you wish to receive coverage
- your device location

We use and disclose this information to:

- communicate your health information, or the health information of someone you are caring for, to health care providers treating you or the other person
- communicate to you the health information of others you are authorized to act on behalf of on the Site
- help you pay for prescription refills or medical bills
- help you apply for Kaiser Permanente coverage
- send you requested product or service information

- respond to customer service requests
- administer your account
- send you newsletters, voice messages, text messages or email communications
- respond to your questions and concerns
- improve our Site and marketing efforts
- conduct internal quality improvement or business analysis
- customize your experience on the Site, including the display of location-based information that's relevant to your care and how to find care
- de-identify the information in accordance with HIPAA and/or other applicable law

When you provide us with personal information about dependents and family members, we will only use this information for the specific reason for which it is provided. Any personal information you provide us when seeking health insurance or coverage is a voluntary submission of that information under applicable law.

2. Web logs

As is true of most websites, we gather certain information automatically. We maintain standard Web logs that record data about all visitors and customers who use the Site and we store this information for no longer than reasonably useful to carry out its legitimate business purpose, or as legally required. These logs may contain the Internet domain from which you access the Site (such as xfinity.com, att.com, etc.); the IP address which is automatically assigned to your computer when you get on the Internet (a static IP address may be identifiable as being connected to you, while a dynamic address is usually not identifiable); the type of browser and operating system you use; the date and time you visited; the pages or mobile screens you viewed; and the address of the website you linked from, if any. If you sign on to the Site to use secured features, our web logs will also contain an individual identifier and show the services you have accessed.

All Web logs are stored securely, and may only be accessed by Kaiser Permanente employees or designees on a need-to-know basis for a specific purpose. Kaiser Permanente uses Web log information to help us design our Site, to identify popular features, to resolve user, hardware, and software problems, to make the Site more useful to visitors and for security purposes.

3. Internet cookies

We and our service providers may place Internet "cookies" or similar technologies (JavaScript, HTML5, ETag) on the computer hard drives of visitors to the Site. Information we obtain helps us to tailor our Site to be more helpful and efficient for our visitors. For example, we are able to see the navigation path taken by users, and that information allows us to understand user success or challenges with the web experience. The cookie consists of a unique identifier that does not contain information about your health history. We use two types of cookies, "session" cookies and "persistent" cookies, along with other similar technologies.

A session cookie is temporary, and expires after you end a session and close your web or app browser. We use session cookies to help customize your experience on our Site, maintain your signed-on status as you navigate through our features, and to track your "click path" through our web pages or mobile screens.

Persistent cookies remain on your hard drive after you've exited from our Site, and we use them for several reasons. For instance, if you've given us permission to email you with information about your Kaiser Permanente benefits, or for other reasons, we may place a persistent cookie on your hard drive that will let us know when you come back to visit our Site. We sometimes use this type of persistent cookie with a "Web beacon" (see below). Persistent cookies will not contain any personal health information about you such as a Kaiser Permanente Health/Medical Record number.

You may have software on your computer that will allow you to decline or deactivate Internet cookies, but if you do so, some features of the Site may not work properly for you. For instructions on how to remove cookies from your hard drive, go to your browser's website for detailed instructions. In addition, further information regarding cookies may be available on other websites or from your Internet service provider. Safari, Chrome, Firefox, Internet Explorer and iOS browsers are commonly used browsers.

4. Web beacons

We may also occasionally use "Web beacons" (also known as "clear gifs," "Web bugs," "1-pixel gifs," etc.) that allow us to collect non-personal information about your response to our email communications, and for other purposes. Web beacons are tiny images, placed on a Web page or email, that can tell us if you've gone to a particular area on our Site. For example, if you've given us permission to send you emails, we may send you an email urging you to use a certain feature on our Site. If you do respond to that email and use that feature, the Web beacon will tell us that our email communication with you has been successful. We do not collect any personal health information with a Web beacon, and do not link Web beacons with any other personal health information you've given us.


Since Web beacons are used in conjunction with persistent cookies (described above), if you set your browser to decline or deactivate cookies, Web beacons cannot function.

Our mobile application contains software development kits (SDKs) that may collect and transmit information back to us or third-party partners about your usage of that mobile application or other applications on your device. Such data, when collected by a 3rd party, that may show what click path was taken, what pages users visited and how long certain pages took to display, is not identifiable to you as an individual.

5. Re-targeting

We have contracted a third party ad network to manage our advertising on other sites. Our ad network service provider uses cookies, Web beacons, and other tracking technologies to

collect information about your activities on this and other websites and to then provide you with KP advertising on other websites. We may also place a persistent third-party cookie (provided by Google) on your hard drive if you sign on to kp.org. This cookie will prevent kp.org members from seeing advertising that is targeted towards people who are not members of Kaiser Permanente's health plan, when searching on Google.

If you wish to not have this information used for the purpose of serving you targeted ads, [you may opt out](#) . Please note this does not opt you out of being served advertising. You may continue to receive generic non-targeted ads.

6. Emails, voice messages, and SMS text messaging

Kaiser Permanente may use a third-party vendor to help us manage some of our email and voice/text messaging communications with you. While we do supply these vendors with email addresses or mobile telephone numbers of those we wish for them to contact, your email address or mobile telephone number is never used for any purpose other than to communicate with you on our behalf. When you click on a link in an email, you may temporarily be redirected through one of the vendor's servers (although this process will be invisible to you) which will register that you've clicked on that link, and have visited our Site. Kaiser Permanente never shares any information, other than your email address or telephone number, with our third-party email and voice/text messaging vendors, which may only share this information with its authorized subcontractors.

At any time, and even if you have expressly given us permission to send voice/text messages to you, you may communicate your desire not to receive additional voice/text messages by following the stop or opt-out instructions in the voice or text message, by adjusting your preferences on kp.org (for only certain categories of communications), or by contacting Member Services.

7. Evaluation and quality improvement

We will periodically ask users to complete surveys asking about their experiences with features of the Site. Our surveys ask visitors for demographic information such as age, gender, and education, but will not request that users provide specific information about any medical condition. We use survey information for evaluation and quality improvement purposes, including helping Kaiser Permanente to improve information and services offered through the Site. In addition, users giving feedback may be individually contacted for follow-up due to concerns raised during the course of such evaluation. Demographic information and Web log data may be stored for future evaluation and quality improvement activities.

8. Application for Kaiser Permanente membership

If you apply for Kaiser Permanente membership through the Site, you will be asked during the application process to disclose certain personal information so that we can evaluate

your eligibility, and you will be asked to verify the truthfulness of your answers.

9. Messages and transactions

Comments or questions sent to us using email or secure messaging forms will be shared with Kaiser Permanente staff and health care professionals who are most able to address your concerns. We will archive your messages once we have made our best effort to provide you with a complete and satisfactory response.

Some of our services such as our automated appointment selection and prescription refill services interact directly with other Kaiser Permanente data systems. Data about your transaction may be stored in these systems, and available to people who test and support these systems.

When you use a service on the secure section of the Site to interact directly with Kaiser Permanente health care professionals, some information you provide may be documented in your medical record, and available for use to guide your treatment as a patient.

10. Credit card transactions

If you provide us with your credit card number for pharmacy prescriptions or other payments, we will treat your credit card number in a secure manner.

11. Data integrity and correction

You have the right to request to view and correct personal information from the Site. Such requests may be submitted using the contact information in the "Questions, complaints, and contacts" section below.

If your personal information changes, you have the right to update or request deletion of information collected on our Site, or if you believe a third party has provided us with your personal information and you would like to request that it be edited or removed from our database, please use the contact information in the "Questions, complaints, and contacts" section below. We will respond to all access requests within 30 days.

12. Children

We do not knowingly collect personally identifiable information from children under the age of 13. If Kaiser Permanente is made aware of collecting information from a child under 13, we will delete this information.

13. Disclosures

We may disclose personal information to any person performing audit, legal, operational, or other services for us. We will use information which does not identify the individual for these activities whenever reasonably possible. Information disclosed to vendors or contractors for operational purposes may not be re-disclosed to others by such a vendor or contractor, except as permitted by KP and applicable law.

We may also disclose your personal information to third parties who provide services on our behalf to help with our business activities. These companies are authorized to use your personal information only as necessary to provide these services to us pursuant to written instructions. In such cases, these companies must abide by our data privacy and security requirements, and are not allowed to use your personal information they receive from us for any other purpose.

These services may include:

- payment processing
- providing customer service
- sending marketing communications
- fulfilling subscription services
- conducting research and analysis
- providing cloud computing infrastructure

We may also disclose your personal information:

- as required by law, such as to comply with a subpoena, or similar legal process
- as described in our Notices of Privacy Practices for protected health information
- when we believe in good faith that disclosure is necessary to protect our rights, protect you or others safety from threats of imminent harm, investigate fraud or other activity in violation of the law, or respond to lawful request by public authorities (including to meet national security or law enforcement requirements)
- to protect the security and reliability of the Site
- if Kaiser Permanente is involved in a merger, acquisition, or sale of all or a portion of its assets. You will be notified via email and/or a prominent notice on our Site of any change in ownership or uses of your personal information, as well as any choices you may have regarding your personal information
- to any other third party with your prior consent to do so
- to Kaiser Permanente entities to carry out business planning and development and business management and general administrative activities, such as to provide, maintain and personalize our sites and services, and to communicate with you

14. Opt out

If a user makes a request to receive information (for example, requesting a subscription to one of our online publications) in an ongoing manner through the Site by providing an email address or mobile phone number the user may request to discontinue future mailings or messages. Similarly, if you receive information about a Kaiser Permanente service through

email or voice/text message, you may make a request to discontinue receiving similar messages in the future. Materials sent to you by email or voice/text message may contain information about how to opt out. Please note, however, that you cannot opt out of certain messages, such as an email letting you know that a doctor has sent you a secure message, or our Partners in Health newsletter. For more information regarding what email communications are considered essential for registered Website members, and for which you cannot opt-out of, please review the Site Terms and Conditions.

Also, if as a member you register to use protected features on our Site, you may be given an opportunity to receive emails, voice or text messages about different types of Kaiser Permanente products, services, announcements, and updates. On our Site, you may change your preferences by clicking "my profile" at the top right of each page, then choosing "communication preferences" on the left.

15. Other requests to limit use and disclosure of your personal information

State and federal laws may allow you to request that we limit our uses and disclosures of your personal information for treatment, payment, and health care operations purposes. We will consider all requests and, if we deny your request, we will notify you in writing. Federal law requires us to agree to your request to restrict disclosures to a health plan or insurer relating to specific health care services, if you have paid for those services in full. The law does not, however, require us to restrict any disclosures we think are important for treatment purposes.

16. Data retention

We will retain your personal information for the period necessary to fulfill the purposes outlined in this Privacy statement, including to meet our legal obligations, resolve disputes, and enforce our agreements, unless a longer retention period is required or permitted by law.

17. Social media

Our Site includes Social Media Features, such as the Facebook button. These Features may collect your IP address, which page you are visiting on our Site, and may set a cookie to enable the Feature to function properly. Social Media Features are either hosted by a third party or hosted directly on our Site. Your interactions with these Features are governed by the privacy statement of the company providing them.

18. Links to third party websites

Our Site includes links to other websites whose privacy practices may differ from those of Kaiser Permanente. If you submit personal information to any of those sites, your information is governed by their privacy statements. We encourage you to carefully read the privacy statement of any website you visit.

19. Location

An IP address (also called Internet address) is assigned to your device by your Internet Service Provider, and is a requirement to use the internet. IP addresses are used to make the connection between your device and the websites and services you use. You can't prevent a website or app from getting the IP address of your device. Your IP address includes some general information about your device location and we use that to display your proximate location in the website and mobile app user experience. We derive your internet device's proximate location from your IP address, which is provided to us when you come to the Site. We do this to provide you with a customized experience on our Site, including the display of location-based information that's relevant to you and your care.

With your permission, we may collect your precise device location using technologies like GPS, Wi-Fi, and Bluetooth, to help you find a facility, doctor, or directions within a facility or to provide you with timely notices when you visit a facility.

Please note that in the App, you may opt in or out of location-based services by editing the App location setting at the device level. For additional information regarding how to do this on your device, please contact us by sending a message to the [Kaiser Permanente Web manager](#).

20. Third party applications

At your request, we may send your personal information to apps that are created and owned by a third party. Kaiser Permanente does not control the app or app provider and is not responsible for the integrity, privacy, security or breach of data transferred to, or stored in the app, or the use or disclosure of data by the app or the app provider once the data are released by Kaiser Permanente. We encourage you to carefully review the terms of use and privacy policy and settings that apply to the app and the app provider and approve release of data only to those apps and app providers that you trust.

Questions, complaints, and contacts

If you have any questions about this Privacy Statement, our policies and practices concerning the Site, your rights under this statement, and your dealings with the Kaiser Permanente Site, you can contact Kaiser Permanente by telephone at 1-800-556-7677 (toll free), or 711 (toll-free TTY for the hearing/speech impaired), by sending a message to the [Kaiser Permanente Web manager](#), or by U.S. mail at the address below:

Kaiser Permanente, kp.org Privacy
4460 Hacienda Drive, Building A, Third Floor
Pleasanton, CA 94588

Last revised: October 2021

Version 1.8

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

John Doe and Jane Doe

(b) County of Residence of First Listed Plaintiff San Bernardino
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Kessler Topaz Meltzer Check, LLP, One Sansome St., Ste 1850, San Francisco, CA 94104,
(415) 400-3000

DEFENDANTS

Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The Permanente Medical Group, Inc.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

Sheppard, Mullin, Richter & Hampton LLP, 1540 El Camino Real, Ste 120, Menlo Park, CA 90425

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

☐ 1 U.S. Government Plaintiff

☒ 3 Federal Question
(U.S. Government Not a Party)

☐ 2 U.S. Government Defendant

☐ 4 Diversity
(Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input type="checkbox"/> 4
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<div>110 Insurance</div> <div>120 Marine</div> <div>130 Miller Act</div> <div>140 Negotiable Instrument</div> <div>150 Recovery of Overpayment Of Veteran's Benefits</div> <div>151 Medicare Act</div> <div>152 Recovery of Defaulted Student Loans (Excludes Veterans)</div> <div>153 Recovery of Overpayment of Veteran's Benefits</div> <div>160 Stockholders' Suits</div> <div>190 Other Contract</div> <div>195 Contract Product Liability</div> <div>196 Franchise</div>	<div><div>PERSONAL INJURY</div><div>310 Airplane</div><div>315 Airplane Product Liability</div><div>320 Assault, Libel & Slander</div><div>330 Federal Employers' Liability</div><div>340 Marine</div><div>345 Marine Product Liability</div><div>350 Motor Vehicle</div><div>355 Motor Vehicle Product Liability</div><div>360 Other Personal Injury</div><div>362 Personal Injury -Medical Malpractice</div></div> <div><div>PERSONAL INJURY</div><div>365 Personal Injury – Product Liability</div><div>367 Health Care/ Pharmaceutical Personal Injury Product Liability</div><div>368 Asbestos Personal Injury Product Liability</div></div> <div><div>PERSONAL PROPERTY</div><div>370 Other Fraud</div><div>371 Truth in Lending</div><div>380 Other Personal Property Damage</div><div>385 Property Damage Product Liability</div></div> <div><div>CIVIL RIGHTS</div><div>440 Other Civil Rights</div><div>441 Voting</div><div>442 Employment</div><div>443 Housing/ Accommodations</div><div>445 Amer. w/Disabilities– Employment</div><div>446 Amer. w/Disabilities–Other</div><div>448 Education</div></div> <div><div>PRISONER PETITIONS</div><div>HABEAS CORPUS</div><div>463 Alien Detainee</div><div>510 Motions to Vacate Sentence</div><div>530 General</div><div>535 Death Penalty</div><div>OTHER</div><div>540 Mandamus & Other</div><div>550 Civil Rights</div><div>555 Prison Condition</div><div>560 Civil Detainee– Conditions of Confinement</div></div>	<div>625 Drug Related Seizure of Property 21 USC § 881</div> <div>690 Other</div> <div><div>LABOR</div><div>710 Fair Labor Standards Act</div><div>720 Labor/Management Relations</div><div>740 Railway Labor Act</div><div>751 Family and Medical Leave Act</div><div>790 Other Labor Litigation</div><div>791 Employee Retirement Income Security Act</div></div> <div><div>IMMIGRATION</div><div>462 Naturalization Application</div><div>465 Other Immigration Actions</div></div>	<div>422 Appeal 28 USC § 158</div> <div>423 Withdrawal 28 USC § 157</div> <div><div>PROPERTY RIGHTS</div><div>820 Copyrights</div><div>830 Patent</div><div>835 Patent–Abbreviated New Drug Application</div><div>840 Trademark</div><div>880 Defend Trade Secrets Act of 2016</div></div> <div><div>SOCIAL SECURITY</div><div>861 HIA (1395ff)</div><div>862 Black Lung (923)</div><div>863 DIWC/DIWW (405(g))</div><div>864 SSID Title XVI</div><div>865 RSI (405(g))</div></div> <div><div>FEDERAL TAX SUITS</div><div>870 Taxes (U.S. Plaintiff or Defendant)</div><div>871 IRS–Third Party 26 USC § 7609</div></div>	<div>375 False Claims Act</div> <div>376 Qui Tam (31 USC § 3729(a))</div> <div>400 State Reapportionment</div> <div>410 Antitrust</div> <div>430 Banks and Banking</div> <div>450 Commerce</div> <div>460 Deportation</div> <div>470 Racketeer Influenced & Corrupt Organizations</div> <div>480 Consumer Credit</div> <div>485 Telephone Consumer Protection Act</div> <div>490 Cable/Sat TV</div> <div>850 Securities/Commodities/ Exchange</div> <div><input checked="" type="checkbox"/> 890 Other Statutory Actions</div> <div>891 Agricultural Acts</div> <div>893 Environmental Matters</div> <div>895 Freedom of Information Act</div> <div>896 Arbitration</div> <div>899 Administrative Procedure Act/Review or Appeal of Agency Decision</div> <div>950 Constitutionality of State Statutes</div>

V. ORIGIN (Place an "X" in One Box Only)

☒ 1 Original Proceeding

☐ 2 Removed from State Court

☐ 3 Remanded from Appellate Court

☐ 4 Reinstated or Reopened

☐ 5 Transferred from Another District (specify)

☐ 6 Multidistrict Litigation–Transfer

☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
18 U.S.C. §§ 2510, et seq.

Brief description of cause:
Privacy violations of the Electronic Communications Privacy Act, the Constitution of the State of California, the California Invasion of Privacy Act, and common law.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P.

DEMAND \$

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only)

☒ SAN FRANCISCO/OAKLAND

☐ SAN JOSE

☐ EUREKA-MCKINLEYVILLE

DATE 06/09/2023

SIGNATURE OF ATTORNEY OF RECORD /s/ Jennifer L. Joost

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
- c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 - (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
 - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
 - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
 - (1) Original Proceedings. Cases originating in the United States district courts.
 - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
 - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
 - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”

Date and Attorney Signature. Date and sign the civil cover sheet.