Jason S. Hartley, Esq. (SBN 192514)
Jason M. Lindner, Esq. (SBN 211451)
**HARTLEY LLP**
101 West Broadway, Suite 820
San Diego, California 92101
Tel: (619) 400-5822
Email: *hartley@hartleyllp.com*
*lindner@hartleyllp.com*

*Attorneys for Plaintiffs*

**IN THE UNITED STATES DISTRICT COURT**

**FOR THE SOUTHERN DISTRICT OF CALIFORNIA**

EDWARD BARBAT, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

SHARP HEALTHCARE,

Defendant.

Case No. **'23CV0330 RSH AHG**

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Plaintiff Edward Barbat, by and through his undersigned attorneys and on behalf of himself and all others similarly situated, brings this class action for violation of California's Invasion of Privacy Act, Cal. Penal Code § 631 ("CIPA"), violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10 ("CMIA"), invasion of privacy, and breach of fiduciary duty, suffered as a result of Defendant Sharp Healthcare's ("Sharp") disclosure of confidential health care information and other personal information to Meta Platforms Inc., formerly known as Facebook, Inc. ("Facebook") through the incorporation of the Meta Pixel, a hidden advertising tool on Sharp's webpages.

## NATURE OF THE ACTION

1. An investigation by the nonprofit news publication The Markup recently revealed

the prevalence of Facebook's advertising tool, the Meta Pixel,[1] on sensitive websites, including thirty-three of America's top hospitals. Sharp is one of those hospitals.

2. The Meta Pixel is a snippet of internet browser code which sends information from the websites it is on, including personal information, pages viewed, and even information entered into forms, to Facebook for use in advertising purposes.

3. Plaintiff, and other similarly situated individuals, were not informed and did not consent to Sharp sharing their private information with Facebook.

4. By sharing this information, Sharp has violated CIPA, CMIA, its fiduciary duty to Plaintiff and the Class members, and invaded Plaintiff and Class members' privacy.

**PARTIES**

5. Plaintiff Edward Barbat is a resident of San Diego, California. During the Class period, Plaintiff utilized Sharp's website for various activities throughout the Class period such as making payments, scheduling appointments, resetting his password with personal and confidential information, searching for medical specialists, sending personal and confidential messages to health care providers and other related health care matters.

6. Defendant Sharp Healthcare is a "not-for-profit" regional health care group located in San Diego, California and headquartered at 8695 Spectrum Center Blvd, San Diego, CA 9212. Sharp runs four acute-care hospitals, three specialty hospitals, three affiliated medical groups, and bills itself as offering a "full spectrum of other facilities and services."[2]

**JURISDICTION AND VENUE**

7. Subject-matter jurisdiction exists in this Court pursuant to 28 U.S.C. § 1442(a)(1).[3]

8. This Court has jurisdiction over Plaintiffs' state law claims pursuant 28 U.S.C. § 1367 because the state claims are so related to the claims in the action within original jurisdiction

[1] At one point, the tool was known as a Facebook Pixel, but was rebranded along with the company. https://www.digitaltrends.com/social-media/what-is-a-facebook-pixel/

[2] https://www.sharp.com/about/

[3] Sharp has removed two other state court cases based on this statute and Sharp's allegations that it was effectively acting as a federal officer consistent with direction from the government. *See Cousin v. Sharp Healthcare*, Case No. 3:22-cv-02040-MMA-DDL at Dkt. No. 1; *Camus et al. v. Sharp Healthcare*, Case No. 3:22-cv-00033-W-BLM at Dkt. No. 1. Plaintiff does not admit that this defense has any merit, but does not contest that it presents a question suitable for federal adjudication.

that they form part of the same case or controversy.

9. Venue in this district is proper pursuant to 28 U.S.C. §1391 because this District is where Sharp resides, and where the acts giving rise to Plaintiff's and Class members' injuries occurred.

## FACTUAL BACKGROUND

10. Facebook is a social media corporation based in Menlo Park, California. It is one of the world's most valuable companies and is considered to be one of the "Big Five" technology companies, along with Microsoft, Amazon, Apple, and Google.

11. Facebook ranked No. 46 in the 2020 Fortune 500 list of the largest United States corporations by revenue, the vast majority of which comes from advertising. In 2019, Facebook's ad revenues were approximately $69.66 billion USD, accounting for about 98.5 percent of its global revenue.[4]

12. A big portion of Facebook's business involves the use of online analytics. Online analytics services allow website owners, app developers, and advertisers to provide targeted advertising to users by learning more about consumers' usage of their apps, such as how many users opened their app on a particular day or how many purchases were made in the app in a particular period. Website owners and app developers program their software to collect certain data about users, which is then sent to the analytics service. The analytics service then provides the developer with analysis of that usage data, often linked with other data that the analytics service has on a given user. Some companies offer these analytics services for a fee; others, as in the case of Facebook, provide the analytics services free of charge as a way to drive ad revenue on their own related platforms.[5]

13. One tool that Facebook uses to collect data for its online analytics is the Meta Pixel. Facebook describes the Meta Pixel as "a snippet of JavaScript code that allows you to track visitor activity on your website. It works by loading a small library of functions which you can use whenever a site visitor takes an action (called an event) that you want to track (called a

[4] New York State Department of Financial Services Report on Investigation of Facebook Inc. Data Privacy Concerns, February 18, 2021.
[5] *Id.*

conversion). Tracked conversions appear in the Ads Manager where they can be used to measure the effectiveness of your ads, to define custom audiences for ad targeting, for Advantage+ catalog ads campaigns, and to analyze that effectiveness of your website's conversion funnels."[6]

14. According to Facebook, the Meta Pixel can collect anything present in http headers, which include "IP addresses, information about the web browser, page location, document, referrer and person using the website," button click data including "any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks," form field names as well as form field values if selected by the website owner, and other optional values.[7] The Meta Pixel captures at least seventeen standard events including payment info, registration for events, location search information, purchases, scheduling information such as appointments, information that was searched for, applications, and what content was viewed.[8]

15. Facebook touts the "retargeting ability of the Meta Pixel," describing how it can help advertisers create "Custom Audiences," tailoring advertisements to "people who have engaged with the page your pixel is on."[9] It also describes how the information harvested by the Meta Pixel can build "Lookalike Audiences," analyzing the information and generating a similar group for targeting.[10] Lookalike Audiences are intended to "have interests, likes, and demographic stats similar to the people who are already engaging with your website and ads."[11] To do this, Facebook naturally needs to receive and analyze these types of information after they are gathered by the Meta Pixel. Facebook states that "To create a lookalike audience, our system leverages information such as demographics, interests and behaviors from your source audience to find new people who share similar qualities."[12]

16. Facebook recommends that the Meta Pixel be installed "on the back-end of all the relevant pages you want to track, create audiences, and remarket with." As an example, for a sales

[6] https://developers.facebook.com/docs/meta-pixel/
[7] *Id.*
[8] https://www.shopify.com/blog/72787269-relax-advertising-on-facebook-just-got-a-lot-easier
[9] "What is the Meta Pixel & What Does it Do?", Ted Vrountas, Facebook Advertising, https://instapage.com/blog/meta-pixel
[10] *Id.*
[11] https://www.shopify.com/blog/72787269-relax-advertising-on-facebook-just-got-a-lot-easier
[12] https://www.facebook.com/business/m/one-sheeters/facebook-pixel-events

page, it recommends that the Meta Pixel be installed on the post-click landing page, the checkout page, and the "thank you" page after that, to capture information from all segments of the process, and to retarget users who back out of the process early.[13] Because of this, in general, businesses that use the Meta Pixel will have it installed on many pages and locations, not just on a single webpage such as their initial splash page.

17. Facebook's stated policies prohibit app developers and third parties from sending sensitive data to Facebook, such as health related data, or information concerning a user's religious practices or other personal information. However, an investigation by the New York State Department of Financial Services found that "notwithstanding Facebook's policy that app developers should not transmit sensitive data to Facebook, there were many examples where the developers violated that policy and Facebook did indeed — unwittingly, it contends — receive, store, and analyze sensitive data. The information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective at enforcing Facebook's policy or preventing the receipt of sensitive data."[14]

18. In January of 2022, the nonprofit news publication The Markup began investigating the prevalence of the Meta Pixel. It noted that "Few people are aware of how expansively Meta tracks their activities. Through Meta Pixel, for instance, a gambling app might notify Meta that you've registered with a particular email address—whether you have a Facebook account or not. The same tracking can occur as you submit an application for a student loan."[15]

19. To research Meta Pixel's use, The Markup partnered with Mozilla Rally, "a data sharing research platform developed in 2021 by Mozilla in collaboration with researchers at Princeton University…The Rally software runs as a browser extension for Firefox that anyone can install and run to participate in public interest studies. When people join Rally studies, they are informed upfront about the nature of the study and what data will be collected. All Rally users

[13] What is the Meta Pixel & What Does it Do?", Ted Vrountas, Facebook Advertising, https://instapage.com/blog/meta-pixel

[14] New York State Department of Financial Services Report on Investigation of Facebook Inc. Data Privacy Concerns, February 18, 2021.

[15] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

consent to participation."[16]

20. The Markup used Rally to "monitor Meta's pixel tracking mechanism and understand the kinds of information it collects on sites across the web." In so doing, it analyzed Meta Pixel's "events", the packets of data the pixel code sends to Meta's servers. Along with data that a person visited a webpage, it found that Meta tracks submission clicks, button clicks, clicks on other areas of a webpage, the seventeen standard events described in Facebook documentation[17], and other custom events.[18]

21. The Markup also noted that Facebook uses "Advanced Matching." Even if a person is not logged into Facebook, "personal information such as name, email, gender, address, or birth date that a site knows about a visitor or that is entered in forms on the website can be collected and used to connect other event data to the Facebook user.[19]" Accordingly, this personal data gathered by Meta Pixel is shared with Facebook regardless of whether the user can be identified as having a Facebook account.

22. Notably, while The Markup could determine what information was being sent to Facebook, it could not determine what Facebook did with that information after it was received:

> Adams: So even though you were able to tell that these companies were sending sensitive information to Facebook, there's no way to tell if Facebook was actually using that to show people ads.
>
> Fondrie-Teitler: Yeah, that's correct. We could see that it was going and was being received by Facebook servers. But we don't have visibility into what happens after that. It's a black box.[20]

23. Internally, Facebook employees have also been blunt about how poorly the company protects sensitive data. Facebook engineers on the ad and business product team wrote in a 2021 privacy overview, which was leaked to the news publication Vice, "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X

[16] *Id.*
[17] *See* paragraph 14, *supra.*
[18] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[19] *Id.*
[20] https://www.marketplace.org/shows/marketplace-tech/metas-pixel-code-helps-businesses-reach-online-customers-but-shares-sensitive-data-about-them/

data for Y purpose.'?"[21]

24. On June 16, 2022, The Markup revealed that it had tested the websites of Newsweek's top 100 hospitals in America, and found the Meta Pixel tracker on thirty-three of them, "sending Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment."[22]

25. The investigation stated that the Meta Pixel often sent the most private of information from these hospital webpages. For example, for one hospital, "clicking the 'Schedule Online' button on a doctor's page prompted the Meta Pixel to send Facebook the text of the button, the doctor's name, and the search term we used to find her: 'pregnancy termination.'" For another, it sent "the text of the button, the doctor's name, and the condition we selected from a dropdown menu: 'Alzheimer's.'" After creating an account on one site, The Markup found that "Clicking on one button prompted the pixel to tell Facebook the name and dosage of a medication in our health record, as well as any notes we had entered about the prescription. The pixel also told Facebook which button we clicked in response to a question about sexual orientation." [23]

26. Sharp's website, www.sharp.com, was one of the hospital websites listed as containing the Meta Pixel code, and accordingly, sent similar personal and private information to Facebook.[24] Sharp's website provides the ability to search for specific medical providers, schedule appointments, make payments, and conduct other private and confidential medical activities which users would not want carelessly disclosed to a third party.

27. Private, personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

[21] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[22] *Id.*
[23] *Id.*
[24] *Id.*

28. In particular, healthcare information has enormous value. Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, has noted how "Health information is a treasure trove for criminals" because it contains "seven to 10 personal identifying characteristics of an individual."[25] Similarly, Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies, has noted that "[M]edical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[26] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[27] Such information, containing extensive personal identifying characteristics, is also valuable to predatory advertisers.

29. As part of their report, The Markup contacted David Holtzman, a health privacy consultant who previously served as a senior privacy adviser in the U.S. Department of Health and Human Services' Office for Civil Rights, for an opinion. He stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it. I cannot say [sharing this data] is for certain a HIPAA violation. It is quite likely a HIPAA violation."[28]

30. Sharp is a healthcare provider covered by HIPPA, the Health Insurance Portability and Accountability Act of 1996 (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

31. These rules establish national standards for the protection of patient information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the

[25] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon
[26] https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web
[27] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[28] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

32. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information." 45 C.F.R. § 164.502. HIPAA also requires that Sharp implement appropriate safeguards for this information. 45 C.F.R. § 164.530(c)(1).

33. Plaintiff and Class members could not have expected that Sharp would disclose their personal information to Facebook, as they had a reasonable expectation that Sharp would comply with HIPAA.

34. Further, Sharp specifically states, regarding its privacy policy, that "At Sharp, protecting your privacy is imperative. We have strict policies and procedures in place to keep your personal health information private, and every Sharp employee is educated on how to ensure that information remains confidential."[29]

35. Sharp's formal privacy policy explicitly states that written authorization from the patient is required for "Sharp HealthCare related marketing activities", with limited exceptions such as "direct face-to-face communication, if we give you a gift that is of nominal value, or if the marketing activity is to provide you with information about Sharp HealthCare's treatment options or services."[30] Nowhere does this policy disclose that personal information would be disclosed to a third-party advertising service such as Facebook.

36. In Plaintiff's case, he had no idea that his personal, confidential information was being disclosed to Facebook. Even after the report from The Markup, Sharp did not disclose to Plaintiff that Meta Pixel had been operating in secret on its website. It was only after Plaintiff received a letter on February 3, 2023 regarding a January 2023 data breach – which Plaintiff still does not know if it was related to the Meta Pixel or was a separate breach by Sharp of personal information – that Plaintiff further investigated and found out about the report showing Sharp's use of Meta Pixel. Plaintiff has used Sharp's website for such purposes as making payments, scheduling appointments, resetting his password with personal and confidential information,

[29] https://www.sharp.com/patient-rights-privacy/privacy-practices.cfm
[30] https://www.sharp.com/patient/upload/Notice-of-Privacy-Practices_2013-2.pdf

searching for medical specialists, sending personal and confidential messages to health care providers and other related health care matters, and was dismayed to find that his personal information may have been shared with Facebook without his consent.

37. Regarding the report from The Markup, Glenn Cohen, faculty director of Harvard Law School's Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics stated "Almost any patient would be shocked to find out that Facebook is being provided an easy way to associate their prescriptions with their name. Even if perhaps there's something in the legal architecture that permits this to be lawful, it's totally outside the expectations of what patients think the health privacy laws are doing for them."[31]

**CLASS ACTION ALLEGATIONS**

38. Plaintiff seeks relief in his individual capacity and on behalf of all those similarly situated. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings this action on behalf of the following class (the "Class"):

> All California citizens who had their personal information collected within the applicable statute of limitations by the Meta Pixel code installed on any web page owned, maintained, and/or operated by Sharp.

39. Excluded from the class are Defendant, including any subsidiary, affiliate, parent, successor, predecessor, or any entity in which Defendant has a controlling interest; any officer or director of Defendant; any Judge or Magistrate presiding over this action and their immediate families; and Plaintiff and Defendant's counsel of record in this action.

40. The Class includes thousands of persons, making individual actions impracticable. While the exact number of Class members is unknown to Plaintiff at this time, they are easily ascertainable through Sharp's medical and website records, as well as Facebook's records.

41. There are questions of fact and law common to the class that predominate over any

[31] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

questions affecting only individual members. The questions of law and fact common to the class arising from Sharp's actions include, without limitation, the following:

a. Whether Sharp knowingly installed the Meta Pixel code on its website;

b. Whether information collected by the Meta Pixel from Sharp's website was communicated to Facebook and/or other third-party advertisers;

c. Whether Sharp's use of the Meta Pixel communicated information transmitted electronically without the consent of all parties to the communication, in violation of CIPA;

d. Whether Sharp's use of Meta Pixel disclosed medical information without authorization, in violation of CMIA;

e. Whether any of the exceptions allowing for disclosure of medical information under CMIA apply;

f. Whether Sharp's use of Meta Pixel breached its fiduciary duty to Plaintiff and Class members;

g. Whether Sharp's use of Meta Pixel violated Class members' constitutional privacy rights; and

h. Whether Class members are entitled to statutory, actual, or other damages, and the proper measure of such relief.

42. Plaintiff's claims are typical of Class members' claims because they all arise from the same conduct by the same Defendant, causing the same type of injury to Plaintiff and the Class members, under the same legal theories.

43. Plaintiff and his counsel will fairly and adequately protect the identical interests of Class members, and Plaintiff is mindful of his duties and responsibilities as a Class representative. Plaintiff has no interest that conflicts with the interests of the Class.

44. Plaintiff has retained counsel that are experienced in class action litigation, having been appointed by courts as plaintiffs' class counsel in dozens of cases.

45. Class certification is superior to other available methods for fairly and efficiently adjudicating Class members' claims because:

a. There are economies for the Court and the parties from litigating the common issues on a class wide basis instead of on a duplicative individual basis;

b. Few Class members would likely have an interest in individually prosecuting separate actions because each Class member's damage claim is potentially too small to make individual litigation economically viable;

c. Regardless of the size of each Class member's claim, the aggregate volume of their claims—coupled with the economies of scale inherent in litigating similar claims on a common basis—will enable Class counsel to litigate this case on a cost-effective basis;

d. Class treatment is required for optimal deterrence and for limiting the reasonable legal expenses incurred by Class members;

e. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences; and

f. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action.

## LEGAL CLAIMS

## COUNT I

**(Violation of California's Invasion of Privacy Act, Cal. Penal Code § 631)**

46. Plaintiff incorporates all previous paragraphs as if alleged in this Count.

47. Cal. Penal Code § 631(a) provides that: "(a) Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally 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, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning 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; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, 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" is punishable by statutory fines and imprisonment.

48. Plaintiff and Class members communicated their private information electronically – i.e., through a "wire, line, or cable" and sent or received within the state of California – to Sharp, through the use of Sharp's website.[32]

49. Sharp's use of the Meta Pixel communicated this information to Facebook without the consent of all parties to the communication.

50. Sharp's use of the Meta Pixel also aided, agreed with, employed, or conspired with Facebook to communicate that information, without the consent of all parties to the communication.

51. Plaintiff and Class members did not consent to disclosure of their information. As described herein, Sharp did not disclose the use of the Meta Pixel and in fact, published privacy policies which indicated that it would not disclose Plaintiff and Class members' private information.

52. Accordingly, Plaintiff and Class members are entitled to all remedies recoverable under CIPA, including, pursuant to Penal Code § 637.2, the greater of $5,000 per violation or three times the amount of actual damages, to be proven at trial.

## COUNT II

**(Violation of California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10)**

53. Plaintiff incorporates all previous paragraphs as if alleged in this Count.

54. Cal. Civ. Code § 56.10 provides that "A provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization," except in specific instances further specified by the statute.

55. None of the exceptions specified in Civ. Code § 56.10, such as being required to disclose information by a court, board, commission, arbitrator, search warrant, medical examiner, other health care providers, insurers, or otherwise specifically as required by law, apply to Sharp's implementation of the Meta Pixel.

[32] The Ninth Circuit has found CIPA applicable to internet communications, including website tracking. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020).

56. "Medical information" is defined by Cal. Civ. Code § 56.05(j) as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment."

57. "Authorization" as defined by Cal. Civ. Code § 56.11, requires written authorization, separate from any other language on the same page, signed and dated by the patient or other legal representative, which "States the specific uses and limitations on the types of medical information to be disclosed," "States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information," "States the name or functions of the persons or entities authorized to receive the medical information," "States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information," "States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information," and "Advises the person signing the authorization of the right to receive a copy of the authorization."

58. As described herein, Sharp's use of the Meta Pixel on its website disclosed medical information to Facebook, without any authorization by Plaintiff and Class members. Sharp did not disclose the use of the Meta Pixel and in fact, published privacy policies which indicated that it would not disclose Plaintiff and Class members' private information. Sharp never asked for, nor obtained, Plaintiff and class members' written authorization to disclose this information to Facebook.

59. Accordingly, Plaintiff and Class members are entitled to all remedies recoverable under CMIA, including, pursuant to Civil Code § 56.36, $1000 in nominal damages per class member, actual damages to be determined at trial, and pursuant to Civil Code § 56.35, compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorney's fees not to exceed one thousand dollars ($1,000), and the costs of litigation.

**COUNT III**

**(Common-Law Invasion of Privacy)**

60. Plaintiff incorporates all previous paragraphs as if alleged in this Count.

61. Plaintiff and Class members had the right to be free of unwarranted invasion to their privacy, including the privacy of their personal and medical information.

62. Plaintiff and Class members suffered Sharp's invasion of this privacy by Sharp's disclosure of their personal and medical information via the Meta Pixel.

63. As described herein, Plaintiff and Class members had a reasonable expectation of privacy based on HIPAA and Sharp's stated privacy policies, as well as by the inherent nature of confidential medical information.

64. Considering the nature of this medical information, the invasion of privacy was highly offensive and objectionable to a reasonable person.

65. The invasion of Plaintiff and Class members' common-law right to privacy proximately caused them to suffer damages, including mental anguish, suffering, and the loss of the value of their protected medical information.

66. Accordingly, Plaintiff and Class members seek all available damages, including compensatory damages, punitive damages, injunctive and declaratory relief, attorneys' fees, and costs of suit.

**COUNT IV**

**(Constitutional Invasion of Privacy)**

67. Plaintiff incorporates all previous paragraphs as if alleged in this Count.

68. In addition to the common-law tort of intrusion, the California Constitution recognizes a right to privacy applicable to governments and private entities. This constitutional right to privacy was added to article I, section 1 of the California Constitution by a 1972 voter initiative.

69. Plaintiff and Class members had a legally protected privacy interest not to have their personal and/or medical information disseminated without their consent. This privacy interest is recognized by statutes such as HIPAA, CMIA, and CPIA.

70. As described herein, Plaintiff and Class members had a reasonable expectation of privacy based on those statutes and Sharp's stated privacy policies, as well as by the inherent nature of confidential medical information.

71. Plaintiff and Class members suffered Sharp's invasion of this privacy by Sharp's disclosure of their personal and medical information via the Meta Pixel.

72. Sharp's conduct constituted a significant and severe intrusion of Plaintiff and Class members' privacy that invaded an interest fundamental to their personal autonomy and was a genuine, nontrivial invasion of their protected privacy interest that defies a reasonable or sensible explanation or justification.

73. The invasion of Plaintiff and Class members' constitutional right to privacy proximately caused them to suffer damages, including mental anguish, suffering, and the loss of the value of their protected medical information.

74. Accordingly, Plaintiff and Class members seek all available damages, including compensatory damages, punitive damages, injunctive and declaratory relief, attorneys' fees, and costs of suit.

**COUNT V**

**(Breach of Fiduciary Duty)**

75. Sharp occupied a position of advisor or counselor to its patients such that Sharp would reasonably inspire confidence that it would act in good faith and in the best interest of its patients. Accordingly, a fiduciary relationship exists between Sharp and its patients, including Plaintiff and class members.

76. By implementing the Meta Pixel on its website and sharing Plaintiff and Class members' information with Facebook, Sharp failed to act in good faith and solely for the benefit of Plaintiff and class members.

77. Sharp's failure to act solely for the benefit of Plaintiff and Class members was a real and meaningful factor in bringing about their injuries.

78. Sharp's breach of fiduciary duty proximately Plaintiff and Class members to suffer damages, including mental anguish, suffering, and the loss of the value of their protected medical

information.

79. Accordingly, Plaintiff and Class members seek all available damages, including compensatory damages, punitive damages, injunctive and declaratory relief, attorneys' fees, and costs of suit.

WHEREFORE, Plaintiff demands judgment in their favor against Defendant, as follows:

1. That Plaintiff and the Class be awarded statutory, actual, compensatory, and punitive damages from Defendants in an amount according to proof at trial;
2. That Plaintiff and the Class be granted declaratory relief from Defendant, including a finding that Defendant's conduct violated CMIA, CIPA, Plaintiff and Class members constitutional and common law rights to privacy, and its fiduciary duty to Plaintiff and Class members;
3. That Plaintiff and the Class be granted injunctive relief enjoining Sharp from further unauthorized and unlawful disclosure of Plaintiff and Class members' private information;
4. That Plaintiff recover attorneys' fees and the costs of this action, including reasonable attorneys' fees pursuant to Cal. Code Civ. P. § 1021.5 and/or pursuant to any statute alleged herein;
5. That Plaintiff and the Class recover prejudgment interest on all amounts awarded;
4. That the Court issue an order certifying the Class as pleaded pursuant to Fed. R. Civ. P. 23 and appointing Plaintiff as Class representatives and their counsel as Class counsel; and
5. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff and members of the Class hereby request a trial by jury of all issues triable by jury.

Dated: February 17, 2023

Respectfully submitted,

*s/Jason S. Hartley*
Jason S. Hartley
Jason M. Lindner
**HARTLEY LLP**
101 W. Broadway, Ste 820
San Diego, CA 92101
(619) 400-5822
hartley@hartleyllp.com
lindner@hartleyllp.com

*Attorneys for Plaintiffs*