

POTTER HANDY LLP

Mark D. Potter (SBN 166317)

mark@potterhandy.com

James M. Treglio (SBN 228077)

jimt@potterhandy.com

100 Pine St., Ste 1250

San Francisco, CA 94111

Tel: (415) 534-1911

Fax: (888) 422-5191

Attorneys for Plaintiff Catrina Brannon, on behalf of herself and all others similarly situated,

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF RIVERSIDE

CVRI 2403395

CATRINA BRANNON, on behalf of herself and
all others similarly situated,

Plaintiff,

vs.

RANCHO FAMILY MEDICAL GROUP, INC.,
a California Corporation; and DOES 1 through
100, inclusive,

Defendants.

CLASS ACTION

**CLASS COMPLAINT FOR DAMAGES
AND INJUNCTIVE RELIEF (FOR
VIOLATIONS OF:**

- (1) THE CONFIDENTIALITY OF
MEDICAL INFORMATION ACT,
CIVIL CODE §§ 56, *ET SEQ.*); and**
- (2) CALIFORNIA UNFAIR
COMPETITION LAW, Cal. Bus. &
Prof. Code §17200, *et seq.***

DEMAND FOR JURY TRIAL

1 Class Representative Plaintiff Catrina Brannon (“Plaintiff”), by and through her attorneys,
2 individually and on behalf of others similarly situated, alleges upon information and belief as
3 follows:

4 **I.**

5 **INTRODUCTION**

6 1. Under the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.*
7 (hereinafter referred to as the “Act”), Plaintiff and all other persons similarly situated, had a right
8 to keep their personal medical information provided to Defendant Rancho Family Medical Group,
9 Inc. (“Rancho” or “Defendant”) confidential. The short title of the Act states, “The Legislature
10 hereby finds and declares that persons receiving health care services have a right to expect that the
11 confidentiality of individual identifiable medical information derived by health service providers
12 be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for
13 the confidentiality of individually identifiable medical information, while permitting certain
14 reasonable and limited uses of that information.” The Act specifically provides that “a provider of
15 health care, health care service plan, or contractor shall not disclose medical information regarding
16 a patient of the provider of health care or an enrollee or subscriber of a health care service plan
17 without first obtaining an authorization...” Civil Code. § 56.10(a). The Act further provides that
18 “Every provider of health care, health care service plan, pharmaceutical company, or contractor
19 who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall
20 do so in a manner that preserves the confidentiality of the information contained therein. Any
21 provider of health care, health care service plan, pharmaceutical company, or contractor who
22 negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical
23 records shall be subject to the remedies ... provided under subdivisions (b) ... of Section 56.36.”
24 Civil Code § 56.101(a).

25 2. Civil Code § 56.36(b) provides Plaintiff, and all other persons similarly situated, with
26 a private right to bring an action against Defendant for violation of Civil Code § 56.101 by
27 specifically providing that “[i]n addition to any other remedies available at law, any individual may
28 bring an action against any person or entity who has negligently released confidential information

1 or records concerning him or her in violation of this part, for either or both of the following: (1) ...
2 nominal damages of one thousand dollars (\$1,000). In order to recover under this paragraph, *it shall*
3 *not be necessary that the plaintiff suffered or was threatened with actual damages.* (2) The amount
4 of actual damages, if any, sustained by the patient.” (Emphasis added.) Here, the release of
5 information to third parties without so much as a subpoena clearly violates the requirements of this
6 statute.

7 3. This class action is brought on behalf of Plaintiff and a putative class defined as all
8 citizens of the State of California who provided their information to the Rancho Family Medical
9 Group, Inc. (“Rancho”) on or before November 19, 2023, and who received notices from Rancho
10 that their information was compromised (“the “Class,” or the “Class Members”).

11 4. As alleged more fully below, Defendant created, maintained, preserved, and stored
12 Plaintiff and the Class members’ personal medical information onto the Defendant’s computer
13 network, including websites and web applications prior to November 19, 2023. Due to a Data
14 Breach on Defendant’s system, there was an unauthorized release of Plaintiff and the Class
15 members’ confidential medical information that occurred continuously from the time this
16 information was provided by the Class to Defendant, in violation of Civil Code § 56.101 of the Act.

17 5. As alleged more fully below, Defendant created, maintained, preserved, and stored
18 Plaintiff and the Class members’ confidential medical information which were released to
19 unauthorized persons, without Plaintiff and the Class members’ prior written authorization. This act
20 of providing unauthorized access to Plaintiff and the Class Members’ confidential medical
21 information continuously constitutes an unauthorized release of confidential medical information in
22 violation of Civil Code § 56.101 of the Act. Because Civil Code § 56.101 allows for the remedies
23 and penalties provided under Civil Code § 56.36(b), Class Representative Plaintiff, individually and
24 on behalf of others similarly situated, seeks nominal damages of one thousand dollars (\$1,000) for
25 each violation under Civil Code § 56.36(b)(1). Additionally, Class Representative Plaintiff,
26 individually and on behalf of others similarly situated, seeks injunctive relief for unlawful violations
27 of Business and Professions Code §§ 17200, *et seq.*

6. Class Representative Plaintiff does not seek any relief greater than or different from the relief sought for the Class of which Plaintiff is a member. The action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons. Private enforcement is necessary and places a disproportionate financial burden on Class Representative Plaintiff in relation to Class Representative Plaintiff's stake in the matter.

II.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class exceeds the \$25,000 jurisdictional minimum of this Court. The amount in controversy as to the Plaintiff individually and each individual Class member does not exceed \$75,000, including interest and any pro rata award of attorneys' fees, costs, and damages. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of Civil Procedure §§ 395(a) and 395.5 because Defendant is registered and does business in the State of California and in the County of Riverside. Defendant has obtained medical information in the transaction of business in the County of Riverside, which has caused both obligations and liability of Defendant to arise in the County of Riverside.

III.

PARTIES

A. PLAINTIFF

8. Class Representative Plaintiff Catrina Brannon is a resident of California. At all times relevant, Plaintiff was a patient of Defendant who utilized Defendant's website and web application to receive medical treatment from Defendant, and was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Defendant in electronic form was in possession of Defendant, including but not limited to Plaintiff's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, addresses, medical

1 record number, insurance provider, electronic mail address, telephone number, or social security
2 number, or other information that, alone or in combination with other publicly available information,
3 reveals Plaintiff's identity. Since receiving treatment at Defendant's facilities, Plaintiff has received
4 numerous solicitations by mail and phone from third parties at an address and number she only
5 provided to Defendant.

6 9. On a Notice dated March 12, 2024, Plaintiff and the Class were informed by
7 Defendant of "a data security incident involving the potential unauthorized access to your personal
8 information." ("Notice").

9 **B. DEFENDANT**

10 10. Defendant Rancho Family Medical Group, Inc. is a California corporation, with its
11 principal places of business located at 28780 Single Oak Drive, Suite 160, Temecula, CA 92590.
12 At all times relevant, Defendant is a "provider of health care" as defined by Civil Code § 56.05(m).
13 Prior to November 19, 2023, Defendant created, maintained, preserved, and stored Plaintiff and the
14 Class members' individually identifiable medical information onto Defendant's computer network,
15 including but not limited to Plaintiff and the Class members' medical history, mental or physical
16 condition, or treatment, including diagnosis and treatment dates. Such medical information included
17 or contained an element of personal identifying information sufficient to allow identification of the
18 individual, such as Plaintiff and the Class members' names, dates of birth, addresses, medical record
19 numbers, insurance providers, electronic mail addresses, telephone numbers, or social security
20 numbers, or other information that, alone or in combination with other publicly available
21 information, reveals Plaintiff and the Class members' identities.

22 **C. DOE DEFENDANTS**

23 11. The true names and capacities, whether individual, corporate, associate, or otherwise,
24 of Defendants sued herein as DOES 1 through 100, inclusive, are currently unknown to the Plaintiff,
25 who therefore sue the Defendants by such fictitious names under the Code of Civil Procedure § 474.
26 Each of the Defendants designated herein as a DOE is legally responsible in some manner for the
27 unlawful acts referred to herein. Plaintiff will seek leave of court and/or amend this complaint to
28 reflect the true names and capacities of the Defendants designated hereinafter as DOES 1 through

1 100 when such identities become known. Any reference made to a named Defendant by specific
2 name or otherwise, individually or plural, is also a reference to the actions or inactions of DOES 1
3 through 100, inclusive.

4 **D. AGENCY/AIDING AND ABETTING**

5 12. At all times herein mentioned, Defendants, and each of them, were an agent or joint
6 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the
7 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the
8 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized
9 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

10 13. Defendants, and each of them, aided and abetted, encouraged and rendered
11 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the
12 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially
13 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the
14 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its
15 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,
16 and wrongdoing.

17 **IV.**

18 **FACTUAL ALLEGATIONS**

19 **A. The Data Breach**

20 14. On a Notice dated March 12, 2024, Plaintiff and the Class were informed by
21 Defendant of “a data security incident involving the potential unauthorized access to your personal
22 information.” (“Notice”). At no point had Plaintiff and the Class provided any authorization to
23 Defendant to release any medical records to any person on their behalf. Nor was any information
24 sought at this time by any third party by way of a subpoena or request for documents in discovery.

25 15. The Notice went on to say that “On January 11, 2024, KMJ Health Solutions (“KMJ
26 Health”), a third-party technology partner of Rancho Family Medical, informed us that a data
27 security event previously reported as a server outage may have resulted in unauthorized access to
28

1 individuals' personal information. This security event occurred on or around November 19, 2023."
2 ("Data Breach").

3 16. As such, Plaintiff is informed and believes that Defendant regularly gave unrestricted
4 access to third parties to the Personal and Medical Information of Plaintiff and all Class Members
5 for an undetermined period of time prior to November 19, 2023.

6 17. Yet, despite knowing many patients were in danger, Defendant did nothing to warn
7 Class Members until almost four months after the Data Breach occurred. During this time,
8 unauthorized third parties had free reign to surveil and defraud their unsuspecting victims.
9 Defendant proceeded business as usual without giving class members the information they needed
10 to protect themselves against fraud and identity theft.

11 18. It is apparent from the Notice that Defendant stores the personal medical information
12 of the Class Members and released them to unauthorized third parties.

13 19. Defendant failed to adequately safeguard Plaintiff and Class Members' Personal and
14 Medical Information, allowing unauthorized third parties to access this wealth of priceless
15 information for an undetermined period of time prior to November 19, 2023, and possibly
16 continuing to date, without warning the victims, the Class Members, to be on the lookout.

17 20. Defendant failed to spend sufficient resources on making sure that its patients'
18 personal medical information are secure and released only to authorized persons.

19 21. Defendant had obligations created by the Health Insurance Portability and
20 Accountability Act ("HIPAA"), the Confidentiality of Medical Information Act ("CMIA"),
21 reasonable industry standards, its own contracts with its patients and employees, common law, and
22 its representations to Plaintiff and Class members, to keep their Personal and Medical Information
23 confidential and to protect the information from unauthorized access.

24 22. Plaintiff and Class members provided their Personal and Medical Information to
25 Defendant with the reasonable expectation and mutual understanding that it would comply with its
26 obligations to keep such information confidential and secure from unauthorized access.

27 23. Indeed, as discussed below, Defendant promised Plaintiff and Class members that it
28 would do just that.

1 **B. Defendant Expressly Promised to Protect Personal and Medical Information**

2 24. Defendant provides all patients, including Plaintiff and Class members, its Notice of
3 Privacy Practices, which states that:

4 Our Privacy Obligations

5
6 The law requires us to maintain the privacy of certain health information called
7 Protected Health Information (PHI). Protected Health Information is the information
8 that you provide us or that we create or receive about your health care. The law also
9 requires us to provide you with this Notice of our legal duties and privacy practices.
10 When we use or disclose (share) your Protected Health Information, we are required
11 to follow the terms of this Notice or other notice in effect at the time we use or share
the PHI. Finally, the law provides you with certain rights described in this Notice.
Furthermore, we are required to notify you following a breach of unsecured PHI.¹

12 25. Likewise, Defendant's Notice of Privacy Practices also states that:

13 Ways We Can Use and Share Your PHI Without Your Written Permission

14
15 In many situations, we can use and share your PHI for activities that are common in
16 many hospitals and clinics. In certain other situations, which we will describe in
17 Section 4 below, we must have your written permission (authorization) to use and/or
share your PHI. ...²

18 26. Notwithstanding the foregoing assurances and promises, Defendant failed to protect
19 the Personal and Medical Information of Plaintiff and other Class members from releasing their
20 information to unauthorized third parties.

21 27. If Defendant truly understood the importance of safeguarding patients' Personal and
22 Medical Information, it would acknowledge its responsibility for the harm it has caused, and would
23 compensate class members, provide long-term protection for Plaintiff and the Class, agree to Court-
24 ordered and enforceable changes to its policies and procedures, and adopt regular and intensive
25 training to ensure that a Data Breach like this never happens again.

26
27 ¹ Rancho, "Notice of Privacy Practices," Effective Date: August 20, 2022,
<https://ranchofamilymed.com/wp-content/uploads/2023/12/Notice-of-Privacy-Practices-1.pdf>, last visited
28 on June 13, 2024.

² *Id.*

1 28. That information is now in the hands unauthorized third parties who will use it if
2 given the chance. Much of this information is unchangeable and loss of control of this information
3 is remarkably dangerous to consumers.

4 **C. Defendant had an Obligation to Protect Personal and Medical Information under**
5 **Federal and State Law and the Applicable Standard of Care**

6 29. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102). As such, it is
7 required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part
8 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”),
9 and Security Rule (“Security Standards for the Protection of Electronic Protected Health
10 Information), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

11 30. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health*
12 *Information* establishes national standards for the protection of health information.

13 31. HIPAA’s Security Rule or *Security Standards for the Protection of Electronic*
14 *Protected Health Information* establishes a national set of security standards for protecting health
15 information that is held or transferred in electronic form.

16 32. HIPAA requires Defendant to “comply with the applicable standards,
17 implementation specifications, and requirements” of HIPAA “with respect to electronic protected
18 health information.” 45 C.F.R. § 164.302.

19 33. “Electronic protected health information” is “individually identifiable health
20 information . . . that is (i) Transmitted by electronic media; maintained in electronic media.” 45
21 C.F.R. § 160.103.

22 34. HIPAA’s Security Rule requires Defendant to do the following:

- 23 a. Ensure the confidentiality, integrity, and availability of all electronic protected health
24 information the covered entity or business associate creates, receives, maintains, or
25 transmits;
- 26 b. Protect against any reasonably anticipated threats or hazards to the security or
27 integrity of such information;
- 28

- 1 c. Protect against any reasonably anticipated uses or disclosures of such information that
2 are not permitted; and
3 d. Ensure compliance by its workforce.

4 35. HIPAA also required Defendant to “review and modify the security measures
5 implemented . . . as needed to continue provision of reasonable and appropriate protection of
6 electronic protected health information.” 45 C.F.R. § 164.306(e).

7 36. HIPAA also required Defendant to “[i]mplement technical policies and procedures
8 for electronic information systems that maintain electronic protected health information to allow
9 access only to those persons or software programs that have been granted access rights.” 45 C.F.R.
10 § 164.312(a)(1).

11 37. Defendant was also prohibited by the Federal Trade Commission Act (“FTC Act”)
12 (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.”
13 The Federal Trade Commission (“FTC”) has concluded that a company’s failure to maintain
14 reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair
15 practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236
16 (3d Cir. 2015).

17 38. In addition to their obligations under federal and state laws, Defendant owed a duty
18 to Class Members whose Personal and Medical Information was entrusted to Defendant to exercise
19 reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal
20 and Medical Information in its possession from being compromised, lost, stolen, accessed, and
21 misused by unauthorized persons. Defendant owed a duty to Class Members to provide reasonable
22 security, including consistency with industry standards and requirements, and to ensure that its
23 systems, policies, procedures, and the personnel responsible for them, adequately protected the
24 Personal and Medical Information of the Class Members.

25 39. Defendant owed a duty to Class Members whose Personal and Medical Information
26 was entrusted to Defendant to design, maintain, and test its systems, policies, and procedures to
27 ensure that the Personal and Medical Information in Defendant’s possession was adequately secured
28 and protected.

1 40. Defendant owed a duty to Class Members whose Personal and Medical Information
2 was entrusted to Defendant to create and implement reasonable data security practices and
3 procedures to protect the Personal and Medical Information in their possession, including
4 adequately training its employees and others who accessed Personal Information within its computer
5 systems on how to adequately protect Personal and Medical Information.

6 41. Defendant owed a duty to Class Members whose Personal and Medical Information
7 was entrusted to Defendant to implement processes that would detect an unauthorized access in a
8 timely manner.

9 42. Defendant owed a duty to Class Members whose Personal and Medical Information
10 was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

11 43. Defendant owed a duty to Class Members whose Personal and Medical Information
12 was entrusted to Defendant to adequately train and supervise its employees to identify and avoid
13 any phishing emails that make it past its email filtering service.

14 44. Defendant owed a duty to Class Members whose Personal and Medical Information
15 was entrusted to Defendant to disclose if its computer systems and data security practices were
16 inadequate to safeguard individuals' Personal and Medical Information from theft or access by
17 unauthorized third parties because such an inadequacy would be a material fact in the decision to
18 entrust Personal and Medical Information with Defendant.

19 45. Defendant owed a duty to Class Members whose Personal and Medical Information
20 was entrusted to Defendant to disclose in a timely and accurate manner when an unauthorized access
21 occurred.

22 46. Defendant owed a duty of care to Class Members because they were foreseeable and
23 probable victims of any inadequate data security practices.

24 //

25 //

26 //

27 //

28 //

1 **D. A Data Breach like this Results in Debilitating Losses to Consumers**

2 47. Each year, identity theft causes tens of billions of dollars of losses to victims in the
3 United States.³ Unauthorized third parties can leverage Plaintiff and Class members' Personal and
4 Medical Information that was obtained in the Data Breach to commit thousands-indeed, millions-of
5 additional crimes, including opening new financial accounts in Class Members' names, taking out
6 loans in Class Members' names, using Class Members' names to obtain medical services and
7 government benefits, using Class Members' Personal Information to file fraudulent tax returns,
8 using Class Members' health insurance information to rack up massive medical debts in their names,
9 using Class Members' health information to target them in other phishing and hacking intrusions
10 based on their individual health needs, using Class Members' information to obtain government
11 benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses
12 in Class Members' names but with another person's photograph, and giving false information to
13 police during an arrest. Even worse, Class Members could be arrested for crimes identity thieves
14 have committed.

15 48. Personal and Medical Information is such a valuable commodity to identity thieves
16 that once the information has been compromised, criminals often trade the information on the cyber
17 black-market for years.

18 49. This is not just speculative. As the FTC has reported, if unauthorized third parties get
19 access to Personal and Medical Information, they *will* use it.⁴

20 50. Unauthorized third parties may not use the information right away. According to the
21 U.S. Government Accountability Office, which conducted a study regarding data breaches:
22 [I]n some cases, stolen data may be held for up to a year or more before being used
23 to commit identity theft. Further, once stolen data have been sold or posted on the
24 Web, fraudulent use of that information **may continue for years**. As a result, studies

25 ³ "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., [https://www.iii.org/fact-](https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime)
26 [statistic/facts-statistics-identity-theft-and-cybercrime](https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime) (discussing Javelin Strategy & Research's report
27 "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

28 ⁴ Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017),
<https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

1 that attempt to measure the harm resulting from data breaches cannot necessarily rule
2 out all future harm.⁵

3 51. Medical identity theft is one of the most common, most expensive, and most difficult
4 to prevent forms of identity theft. According to Kaiser Health News, “medical-related identity theft
5 accounted for 43 percent of all identity thefts reported in the United States in 2013,” which is
6 more “than identity thefts involving banking and finance, the government and the military, or
7 education.”⁶

8 52. “Medical identity theft is a growing and dangerous crime that leaves its victims with
9 little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum.
10 “Victims often experience financial repercussions and worse yet, they frequently discover erroneous
11 information has been added to their personal medical files due to the thief’s activities.”⁷

12 53. As indicated by Jim Trainor, second in command at the FBI’s cyber security division:
13 “Medical records are a gold mine for criminals—they can access a patient’s name, DOB, Social
14 Security and insurance numbers, and even financial information all in one place. Credit cards can
15 be, say, five dollars or more where PHI can go from \$20 say up to—we’ve seen \$60 or \$70
16 [(referring to prices on dark web marketplaces)].”⁸ A complete identity theft kit that includes health
17 insurance credentials may be worth up to \$1,000 on the black market.⁹

18 54. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been
19 placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity
20 theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential
21

22 ⁵ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full*
23 *Extent Is Unknown*, GAO, July 5, 2007, <https://www.gao.gov/assets/270/262904.html> (emphasis added).

24 ⁶ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014,
<https://khn.org/news/rise-of-identity-theft/>.

25 ⁷ *Id.*

26 ⁸ ID Experts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, New Ponemon
27 *Study Shows*, [https://www.idexperts.com/knowledge-center/single/you-got-it-they-want-it-criminals-](https://www.idexperts.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat)
[are-targeting-your-private-healthcare-dat](https://www.idexperts.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat)

28 ⁹ *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from
The Global State of Information Security Survey 2015, [https://www.pwc.com/gx/en/consulting-](https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf)
[services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf](https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf)

1 impact of the Data Breach on their everyday lives, including placing “freezes” and “alerts” with
2 credit reporting agencies, contacting their financial institutions, healthcare providers, closing or
3 modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports,
4 and health insurance account information for unauthorized activity for years to come.

5 55. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which
6 they are entitled to compensation, including:

- 7 a. Trespass, damage to, and theft of their personal property including Personal and
8 Medical Information;
- 9 b. Improper disclosure of their Personal and Medical Information;
- 10 c. The imminent and certainly impending injury flowing from potential fraud and
11 identity theft posed by their Personal and Medical Information being placed in the
12 hands of criminals and having been already misused;
- 13 d. The imminent and certainly impending risk of having their confidential medical
14 information used against them by spam callers to defraud them;
- 15 e. Damages flowing from Defendant’s untimely and inadequate notification of the Data
16 Breach;
- 17 f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing
18 unauthorized third parties have their Personal and Medical Information and that fraudsters
19 have already used that information to initiate spam calls to members of the Class;
- 20 g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time
21 reasonably expended to remedy or mitigate the effects of the Data Breach;
- 22 h. Ascertainable losses in the form of deprivation of the value of customers’
23 personal information for which there is a well-established and quantifiable national and
24 international market;
- 25 i. The loss of use of and access to their credit, accounts, and/or funds;
- 26 j. Damage to their credit due to fraudulent use of their Personal and Medical
27 Information; and
28

1 k. Increased cost of borrowing, insurance, deposits and other items which are adversely
2 affected by a reduced credit score.

3 56. Moreover, Plaintiff and Class have an interest in ensuring that their information,
4 which remains in the possession of Defendant, is protected from further unauthorized release by the
5 implementation of security measures and safeguards.

6 57. Even if Defendant would acknowledge the harm caused by the Data Breach by
7 recommending that Plaintiff and Class Members review the statements they receive from their
8 healthcare providers and health insurer, any amount of identity theft repair and monitoring is
9 woefully inadequate to protect Plaintiff and Class members from a lifetime of identity theft risk and
10 worse, it does nothing to reimburse Plaintiff and Class members for the injuries they have already
11 suffered.

12 V.

13 **CLASS ACTION ALLEGATIONS**

14 58. Class Representative Plaintiff brings this action on her own behalf and on behalf of
15 all other persons similarly situated. The putative class that Class Representative Plaintiff seeks to
16 represent is composed of:

17 All citizens of the State of California who provided their information to the Rancho
18 Family Medical Group, Inc. (“Rancho”) on or before November 19, 2023, and who
19 received notices from Rancho that their information was compromised (hereinafter
20 the “Class”).

21 Excluded from the Class are the natural persons who are directors, and officers, of the
22 Defendant, as well as Plaintiff’s counsel, judges, clerks, and other supporting staff of the Superior
23 Court of California by and for the County of Alameda. Class Representative Plaintiff expressly
24 disclaims that she is seeking a class-wide recovery for personal injuries attributable to Defendant’s
25 conduct.

26 59. Plaintiff is informed and believes that the members of the Class are so numerous that
27 joinder of all members is impracticable. While the exact number of the Class members is unknown
28 to Class Representative Plaintiff at this time, such information can be ascertained through

1 appropriate discovery, from records maintained by Defendant. It is estimated that around 10,000
2 people were affected by this Data Breach.

3 60. There is a well-defined community of interest among the members of the Class
4 because common questions of law and fact predominate, Class Representative Plaintiff's claims are
5 typical of the members of the class, and Class Representative Plaintiff can fairly and adequately
6 represent the interests of the Class.

7 61. Common questions of law and fact exist as to all members of the Class and
8 predominate over any questions affecting solely individual members of the Class. Among the
9 questions of law and fact common to the Class are:

- 11 (a) Whether Defendant failed to adequately safeguard Plaintiff and the Class's Personal
and Medical Information;
- 12 (b) Whether the type of information involved in the Data Breach constitutes confidential
medical information as defined by Civil Code §56.05(j);
- 13 (c) Whether Defendant failed to protect Plaintiff and the Class's Personal and Medical
14 Information;
- 15 (d) Whether the Data Breach violated the FTC Act, HIPAA, CMIA, and/or Defendant's
other duties;
- 16 (e) Whether Defendant violated the data security statutes and notification statutes
17 applicable to Plaintiff and the Class;
- 18 (f) Whether Defendant failed to notify Plaintiff and members of the Class about the Data
Breach expeditiously and without unreasonable delay after the Data Breach was
19 discovered;
- 20 (g) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to
safeguard Class Members' Personal and Medical Information properly and as
21 promised;
- 22 (h) Whether Defendant entered into implied contracts with Plaintiff and the members of
the Class that included contract terms requiring Defendant to protect the
23 confidentiality of Personal and Medical Information and have reasonable security
measures;
- 24 (i) Whether Defendant violated the consumer protection statutes and state medical
privacy statutes applicable to Plaintiff and the Class;
- 25 (j) Whether Defendant's conduct described herein constitutes a breach of their implied
26 contracts with Plaintiff and the Class;
- 27 (k) Whether Plaintiff and the members of the Class are entitled to damages as a result of
Defendant's wrongful conduct;
- 28 (l) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

1 (m) What injunctive relief is appropriate to redress the imminent and currently ongoing
2 harm faced by Plaintiff and members of the Class.

3
4 Class Representative Plaintiff's claims are typical of those of the other Class members because Class
5 Representative Plaintiff, like every other Class member, was exposed to virtually identical conduct
6 and is entitled to nominal damages of one thousand dollars (\$1,000) per violation pursuant to Civil
7 Code §§ 56.101 and 56.36(b)(1).

8 62. Class Representative Plaintiff will fairly and adequately protect the interests of the
9 Class. Moreover, Class Representative Plaintiff has no interest that is contrary to or in conflict with
10 those of the Class she seeks to represent during the Class Period. In addition, Class Representative
11 Plaintiff has retained competent counsel experienced in class action litigation to further ensure such
12 protection and intend to prosecute this action vigorously.

13 63. The prosecution of separate actions by individual members of the Class would create
14 a risk of inconsistent or varying adjudications with respect to individual members of the Class,
15 which would establish incompatible standards of conduct for the Defendant in the State of California
16 and would lead to repetitious trials of the numerous common questions of fact and law in the State
17 of California. Class Representative Plaintiff knows of no difficulty that will be encountered in the
18 management of this litigation that would preclude its maintenance as a class action. As a result, a
19 class action is superior to other available methods for the fair and efficient adjudication of this
20 controversy.

21 64. Proper and sufficient notice of this action may be provided to the Class members
22 through direct mail.

23 65. Moreover, the Class members' individual damages are insufficient to justify the cost
24 of litigation, so that in the absence of class treatment, Defendant's violations of law inflicting
25 substantial damages in the aggregate would go unremedied without certification of the Class.
26 Absent certification of this action as a class action, Class Representative Plaintiff and the members
27 of the Class will continue to be damaged by the unauthorized release of their individual identifiable
28 medical information.

1 VI.

2 **CAUSES OF ACTION**

3 **FIRST CAUSE OF ACTION**

4 **(Violations of the Confidentiality of Medical Information Act, Civil Code § 56, *et seq.*)**
5 (Against All Defendants)

6 66. Plaintiff and the Class incorporate by reference all of the above paragraphs of this
7 Complaint as though fully stated herein.

8 67. Defendant is a “provider of health care,” within the meaning of Civil Code §
9 56.05(m), and maintained and continues to maintain “medical information,” within the meaning of
10 Civil Code § 56.05(j), of “patients” of the Defendant, within the meaning of Civil Code § 56.05(k).

11 68. Plaintiff and the Class are “patients” of Defendant within the meaning of Civil Code
12 § 56.05(k). Furthermore, Plaintiff and the Class, as patients of Defendant, had their individually
13 identifiable “medical information,” within the meaning of Civil Code § 56.05(j), stored onto
14 Defendant’s server, and received treatment at one of Defendant’s hospital, satellite, or urgent care
15 locations on or before November 19, 2023. Plaintiff and the Class also utilized Defendant’s website
16 and/or web application to research medical conditions, make appointments with their physicians for
17 specific medical conditions, email their physicians regarding medical questions they had, amongst
18 other medical uses.

19 69. In a Notice dated March 12, 2024, Plaintiff and the Class were informed by
20 Defendant “of a data security incident involving the potential unauthorized access to your personal
21 information.” Plaintiff and the Class’s individual identifiable “medical information,” within the
22 meaning of Civil Code § 56.05(j),¹⁰ including “name, date of birth, hospital medical record number,
23 hospital treatment location, date of service, and procedure medical code.”
24

25 ¹⁰ Pursuant to Civil Code § 56.05(j), “Medical information” means “any individually identifiable
26 information, in electronic or physical form, in possession of or derived from a provider of health
27 care...regarding a patient’s medical history, mental or physical condition, or treatment. ‘Individually
28 Identifiable’ means that the medical information includes or contains any elements of personal identifying
information sufficient to allow identification of the individual, such as the patient’s name, address,
electronic mail address, telephone number, or social security number, or other information that, alone or in
combination with other publicly available information, reveals the individual’s identity.”

1 70. Despite realizing the Data Breach of Plaintiff’s personal medical information,
2 Defendant took almost four months to inform Plaintiff and the Class of the Data Breach, that allowed
3 unauthorized individual(s) access to Plaintiff and the Class Members’ personal medical information.

4 71. As a result of Defendant’s above-described conduct, Plaintiff and the Class have
5 suffered damages from the Data Breach of their individual identifiable “medical information” made
6 unlawful by Civil Code §§ 56.10 and 56.101.

7 72. Because Civil Code § 56.101 allows for the remedies and penalties provided under
8 Civil Code § 56.36(b), Plaintiff individually and on behalf of the Class seeks nominal damages of
9 one thousand dollars (\$1,000) for each violation under Civil Code § 56.36(b)(1); and Plaintiff
10 individually seeks actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2).

11
12 **SECOND CAUSE OF ACTION**
13 **(Violations of the CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code**
14 **§17200, *et seq.*)**

14 73. Plaintiff incorporates by reference all allegations of the preceding paragraphs as
15 though fully set forth herein.

16 74. Defendant is organized under the laws of California. Defendant violated California’s
17 Unfair Competition Law (“UCL”), Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful,
18 unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading
19 advertising that constitute acts of “unfair competition” as defined in the UCL, including, but not
20 limited to, the following:

- 21 a. by representing and advertising that it would maintain adequate data privacy and
22 security practices and procedures to safeguard their Personal and Medical
23 Information from unauthorized disclosure, release, data breach, and theft;
24 representing and advertising that they did and would comply with the
25 requirement of relevant federal and state laws pertaining to the privacy and
26 security of the Class’ Personal and Medical Information; and omitting,
27 suppressing, and concealing the material fact of the inadequacy of the privacy
28 and security protections for the Class’ Personal and Medical Information;

- 1 b. by soliciting and collecting Class members' Personal and Medical Information
2 with knowledge that the information would not be adequately protected; and by
3 storing Plaintiff and Class members' Personal and Medical Information in
4 an unsecure environment;
- 5 c. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d,
6 *et seq.*; and
- 7 d. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*

8 75. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous,
9 unconscionable, and/or substantially injurious to Plaintiff and Class members. Defendant's practice
10 was also contrary to legislatively declared and public policies that seek to protect consumer data and
11 ensure that entities who solicit or are entrusted with personal data utilize appropriate security
12 measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et*
13 *seq.*, and the CMIA, Cal. Civ. Code § 56, *et seq.*

14 76. As a direct and proximate result of Defendant's unfair and unlawful practices and
15 acts, Plaintiff and the Class were injured and lost money or property, including but not limited to
16 the overpayments Defendant received to take reasonable and adequate security measures (but did
17 not), the loss of their legally protected interest in the confidentiality and privacy of their Personal
18 and Medical Information, and additional losses described above. In addition, Defendant treated the
19 personal and medical information of Plaintiff and the Class as its own property, and sold it for profit,
20 causing a loss of money and property to Plaintiff and the Class.

21 77. Defendant knew or should have known that Data Breach would violate the CMIA,
22 HIPAA and the FTC, and would fail to safeguard Plaintiff and Class members' Personal and
23 Medical Information. Defendant's actions in engaging in the above-named unfair practices and
24 deceptive acts were intentional, knowing and willful, and/or wanton and reckless with respect to the
25 rights of the Class.

26 78. The conduct and practices described above emanated from California where
27 decisions related to Defendant's advertising and data security were made.

28

79. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired, including all monies it received through the sale of this medical information, by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the Court to grant Plaintiff and the Class members the following relief against Defendant:

a. An order certifying this action as a class action under Code of Civil Procedure §382, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, including statutory damages under the CMIA, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein, including, but not limited to:

- i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

- 1 iv. Ordering that Defendant’s segment customer data by, among other things,
2 creating firewalls and access controls so that if one area of Defendant’s
3 systems is compromised, hackers cannot gain access to other portions of
4 Defendant’s systems;
5 v. Ordering that Defendant purge, delete, and destroy in a reasonably secure
6 manner customer data not necessary for its provisions of services;
7 vi. Ordering that Defendant conduct regular database scanning and securing
8 checks;
9 vii. Ordering that Defendant routinely and continually conduct internal training
10 and education to inform internal security personnel how to identify and
11 contain a Data Breach when it occurs and what to do in response to a Data
12 Breach; and
13 viii. Ordering Defendant to meaningfully educate its current, former, and
14 prospective employees and subcontractors about the threats they face as a
15 result of the loss of their financial and personal information to third parties,
16 as well as the steps they must take to protect themselves.;
17 d. An order requiring Defendant to pay the costs involved in notifying the Class
18 members about the judgment and administering the claims process;
19 e. Restitutionary disgorgement of all wrongly acquired monies received by Defendant
20 from the sale of the medical information of Plaintiff and the Class Members, including monies
21 directly received from advertisers;
22 f. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-
23 judgment interest, reasonable attorneys’ fees, costs and expenses as allowable by law, including the
24 UCL, Cal. Bus. & Prof. Code § 17082 and the CMIA, Cal. Civ. Code 56.35; and
25 g. An award of such other and further relief as this Court may deem just and proper.
26
27
28

POTTER HANDY LLP

Dated: June 17, 2024

By: /s/ James M. Treglio
Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiff and the Class

DEMAND FOR JURY TRIAL

Plaintiff and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

POTTER HANDY LLP

Dated: June 17, 2024

By: /s/ James M. Treglio
Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiff and the Class