

JUN 09 2022

Filed _____
BRANDON E. RILEY, CLERK

By _____
Donna Edwards
DEPUTY

1 BETSY C. MANIFOLD (182450)
RACHELE R. BYRD (190634)
2 **WOLF HALDENSTEIN ADLER**
FREEMAN & HERZ LLP
750 B Street, Suite 1820
3 San Diego, California
Telephone: (619) 239-4599
4 Facsimile: (619) 234-4599
manifold@whafh.com
5 byrd@whafh.com

6 SCOTT EDWARD COLE (160744)
LAURA GRACE VAN NOTE (310160)
CODY ALEXANDER BOLCE (322725)
7 **COLE & VAN NOTE**
555 12th Street, Ste. 1725
8 Oakland, CA 94607
Tel.: (510) 891-9800
9 Fax: (510) 891-7030
sec@colevannote.com
10 lvn@colevannote.com
cab@colevannote.com

11 *Co-Lead Counsel for Plaintiffs and the Proposed Class*

12 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
13 **FOR THE COUNTY OF SAN JOAQUIN**

14 DANIEL HINDS, individually and on behalf
of all others similarly situated,

15 Plaintiff,

16 v.

17 COMMUNITY MEDICAL CENTERS, INC.,

18 Defendant.

19 Included Actions:

20 *Beck v. Community Medical Centers, Inc.*
Case No. 2021-10482

21 *Donaire v Community Medical Centers, Inc.*
Case No. 2021-10605

22 *Palermo v. Community Medical Centers, Inc.*
23 Case No. 2021-10626

24 *Miranda v. Community Medical Centers, Inc.*
25 Case No. 2021-11353

Lead Case No.: STK-CV-UNPI-2021-10404
CLASS ACTION

CORRECTED
CONSOLIDATED CLASS ACTION
COMPLAINT FOR:

1. Negligence;
2. Breach of Implied Contract;
3. Breach of Implied Covenant of Good Faith and Fair Dealing;
4. Invasion of Privacy;
5. Unjust Enrichment;
6. Violations of the California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq.*); and
7. Violations of California's Unfair Competition law (Cal. Bus. & Prof. Code § 17200, *et seq.*)

JUDGE: Hon. Erin Guy Castillo
DEPT.: 10B

Filed November 8, 2021

BY FAX

1 **CONSOLIDATED CLASS ACTION COMPLAINT**

2 Plaintiffs Daniel Hinds, Christopher Beck, Mohammad M. Dawood, Sylvia Lopez, Darin
3 Palermo, Aholiva Justiniano Miranda (“Plaintiffs”) bring this Class Action Complaint against
4 Community Medical Centers, Inc. (collectively “Defendant” or “CMC”), individually and on
5 behalf of all others similarly situated (“Class Members”), and allege, upon personal knowledge as
6 to their own actions and their counsel’s investigations, and upon information and belief as to all
7 other matters, as follows:

8 **I. INTRODUCTION**

9 1. Plaintiffs bring this class action against Defendant for its failure to properly secure
10 and safeguard the Protected Health Information (“PHI”)¹, such as medical information of patients,
11 and the Personally Identifiable Information (“PII”)² including, without limitation, first and last
12 names, mailing addresses, dates of birth, Social Security numbers, and demographic information,
13 that Defendant required from patients.

14 2. Defendant is a private non-profit health care system with over 25 facilities across
15 California.³ According to public records, Defendant employed over 1,000 individuals and
16
17

18 ¹ PHI is a category of information that refers to an individual’s medical records and history,
19 which is protected under the Health Insurance Portability and Accountability Act (“HIPAA”) and
20 the California Confidentiality of Medical Information Act, Civil Code § 56, *et seq.* (the “CMIA”).
Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical
21 histories and data points applied to a set of demographic information for a particular patient.

22 ² PII generally incorporates information that can be used to distinguish or trace an
23 individual’s identity, either alone or when combined with other personal or identifying
24 information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly
25 identifies an individual. PII also is generally defined to include certain identifiers that do not on
their face name an individual, but that are considered to be particularly sensitive and/or valuable
if in the wrong hands (for example, Social Security number, passport number, driver’s license
number, financial account number).

³ See <http://www.communitymedicalcenters.org/About-Us> (last visited June 6, 2022);
<http://www.communitymedicalcenters.org/Locations> (last visited June 6, 2022).

1 generated over \$87 million in total revenue in 2020.⁴ Defendant’s patients entrust it with an
2 extensive amount of their PHI/PII. Defendant retains this information for many years.

3 3. Defendant’s “Privacy Policy” on its website, effective as of April 14, 2003,
4 describes the Defendant’s privacy practices and the privacy practices of:

5 all of our doctors, nurses, and other health care professionals authorized to
6 enter information about you into your medical chart[;] all of our departments[;]
7 all of our health center sites[; and] all of our employees, staff, volunteers and
8 other personnel who work for us or on our behalf.⁵

9 The Privacy Policy states that Defendant collects, among other things, PHI, including “health
10 information that identifies you” and “a record of the services that you received.”

11 4. Defendant states that the Privacy Policy applies to all of Defendant’s records about
12 patient care, whether made by Defendant’s health care professionals or others working in
13 Defendant’s office, and tells patients about “the ways in which we may use and disclose your
14 personal health information.”⁶ The Privacy Policy also describes individual’s rights with respect
15 to “the health information that we keep about you and the obligations that we have when we use
16 and disclose your health information.”⁷

17 5. Under “Our Pledge,” the Privacy Policy states that Defendant is “committed to
18 protecting your personal health information” and that Defendant is required by law to:

19 make sure that health information that identifies you is kept private in accordance with
20 relevant law[;] give you this notice of our legal duties and privacy practices with respect to
21 your personal health information[; and] follow the terms of the notice that is currently in
22 effect for all of your personal health information.⁸

23 ⁴ See <https://projects.propublica.org/nonprofits/organizations/942437106> (last visited June
24 6, 2022).

25 ⁵ See Ex. 1 (Defendant’s Privacy Policy) at 1, available at
<http://www.communitymedicalcenters.org/Privacy> (last visited June 6, 2022).

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

1 6. On or around October 10, 2021, Defendant discovered an external system breach
2 that it reports “may have exposed some of [Plaintiffs’] personally identifiable and protected health
3 information” (the “Data Breach”).⁹

4 7. On or around October 26, 2021, Defendant began notifying various states Attorneys
5 General of the Data Breach.

6 8. On October 27, 2021, Defendant posted on its website that “[t]he following personal
7 information could have been compromised by an unauthorized third party: first and last name,
8 mailing address, social security number, date of birth, demographic information, and medical
9 record numbers.”¹⁰

10 9. The forensic audit undertaken to determine the breadth of Defendant’s October
11 2021 Data Breach “confirmed that unauthorized individuals had gained access to parts of its
12 network where protected health information was stored, including first and last names, mailing
13 addresses, dates of birth, Social Security numbers, demographic information, and medical
14 information.”¹¹

15 10. During the Data Breach, the attacker compromised the personal information of
16 more than 656,000 current or former patients of Defendant.¹²

17 11. In late October and early November 2021, Defendant issued a “Notice of Data
18 Breach” to those whose PHI/PII was known to Defendant to have been impacted. Plaintiffs and
19 Class Members received a Notice of Data Breach from Defendant informing them that their
20 PHI/PII was compromised during the Data Breach including their first and last name, mailing
21

22 ⁹ Ex. 2 (sample *Notice of Data Breach* filed with California Attorney General).

23 ¹⁰ See <http://www.communitymedicalcenters.org/News/update-on-recent-network-security-incident-2021> (last visited June 6, 2022).

24 ¹¹ See <https://www.hipaajournal.com/more-than-650k-patients-of-community-medical-centers-notified-about-hacking-incident/> (last visited June 6, 2022).

25 ¹² *Id.*

1 address, Social Security number, date of birth, demographic information, and medical information.

2 12. By obtaining, collecting, using, and deriving a benefit from the PHI/PII of Plaintiffs
3 and Class Members, Defendant assumed legal and equitable duties to those individuals to protect
4 and safeguard that information from unauthorized access and intrusion.

5 13. Hackers access and then offer for sale the unencrypted and unredacted PHI/PII to
6 criminals. The type of exposed PHI/PII of Plaintiffs and Class Members is highly sought after by
7 thieves and is routinely sold on the dark web. Plaintiffs and Class Members face a present and
8 continuing lifetime risk of identity theft, which is heightened here by the loss of PHI and Social
9 Security numbers.

10 14. Defendant failed to adequately protect Plaintiffs' and Class Members' PHI and PII,
11 and failed to encrypt or redact this highly sensitive information.¹³ This was in violation of, *inter*
12 *alia*, required practices, customary practices, and law.

13 15. This unencrypted, unredacted PHI/PII was actually or potentially compromised due
14 to Defendant's negligent and careless acts and omissions and the utter failure to protect the PHI/PII
15 of Plaintiffs and Class Members. Moreover, Defendant has not informed Plaintiffs or Class
16 Members what the specific vulnerabilities and root causes of the Data Breach are.

17 16. Plaintiffs and Class Members are at significant risk of identity theft and various
18 other forms of personal, social, and financial harm. The risk will remain for their respective
19 lifetimes.

21
22 ¹³ See <https://oag.ca.gov/system/files/Community%20Medical%20Centers%20Ad%20r2prf.pdf>
23 (last visited June 6, 2022). It is clear that the information exposed in the Data Breach was
24 unencrypted. California law requires companies to notify California residents “whose
25 **unencrypted** personal information was, or is reasonably believed to have been, acquired by an
unauthorized person” due to a “breach of the security of the system[.]” Cal. Civ. Code §
1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data
Breach on Oct. 26, 2021, evidencing that the exposed data was unencrypted.

1 **II. PARTIES**

2 20. Plaintiff Daniel Hinds (“Plaintiff Hinds”) is an adult individual and, at all relevant
3 times herein, a resident of the State of California, currently residing in Mountain House, California.

4 21. Plaintiff Christopher Beck (“Plaintiff Beck”) is a resident and citizen of California,
5 currently residing in Stockton, California.

6 22. Plaintiff Mohammad M. Dawood (“Plaintiff Dawood”) is a resident and citizen of
7 California, currently residing in Lodi, California.

8 23. Plaintiff Sylvia Lopez (“Plaintiff Lopez”) is a resident and citizen of California,
9 currently residing in Manteca, California.

10 24. Plaintiff Darin Palermo (“Plaintiff Palermo”) is a resident and citizen of California,
11 currently residing in Stockton, California.

12 25. Plaintiff Aholiva Justiniano Miranda (“Plaintiff Miranda”) is a citizen of California
13 currently residing in Stockton, California.

14 26. Defendant Community Medical Centers, Inc. is a California corporation with its
15 principal office located at 7210 Murray Drive, Stockton, California 95210.

16 27. Plaintiffs’ claims stated herein are asserted against Defendant and any of its owners,
17 predecessors, successors, subsidiaries, agents and/or assigns.

18 **III. JURISDICTION AND VENUE**

19 28. This Court has jurisdiction over this action under California Code of Civil
20 Procedure § 410.10. The total amount of damages incurred by Plaintiffs and the Class in the
21 aggregate exceeds the \$25,000 jurisdictional minimum of this Court. Further, the amount in
22 controversy as to Plaintiffs individually does not exceed \$75,000.

23 29. This action does not qualify for federal jurisdiction under the Class Action Fairness
24 Act because the home-state controversy exception under 28 U.S.C. § 1332(d)(4)(B) applies to this

1 action because (1) more than two-thirds of the members of the proposed Class are citizens of the
2 State of California, and (2) Defendant is a citizen of the State of California.

3 30. Venue is proper in this Court under California Bus. & Prof. Code § 17203 and Code
4 of Civil Procedure §§ 395(a) and 395.5, because Defendant is headquartered in this judicial district
5 and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this
6 judicial district.

7 **IV. FACTUAL ALLEGATIONS**

8 ***Background***

9 31. Defendant is a regional medical provider serving patients in Stockton, California
10 and the surrounding region.

11 32. Plaintiffs and Class Members who were patients of Defendant and/or other
12 providers of health care were required to provide sensitive and confidential PHI, including medical
13 information and medical record numbers, and sensitive and confidential PII, including their first
14 and last names, addresses, dates of birth, Social Security numbers, demographic information, and
15 other PII, some of which is static, does not change, and can be used to commit countless different
16 types of financial crimes.

17 33. Plaintiffs and Class Members, as current and former patients of Defendant and/or
18 other providers of health care, relied on the sophistication of Defendant to keep their PHI/PII
19 confidential and securely maintained, to use this information for business purposes only, and to
20 make only authorized disclosures of this information. Plaintiffs and Class Members demand
21 security to safeguard their PHI/PII.

22 34. Defendant had a duty to adopt reasonable measures to protect the PHI/PII of
23 Plaintiffs and Class Members from involuntary disclosure to third parties.

24 ***The Data Breach***

1 35. Beginning on or about October 25, 2021, Defendant sent Plaintiffs and other current
2 and former patients a *Notice of Data Breach*. Defendant informed the recipients of the notice that:

3 **What Happened and What Information Was Involved?**

4 On October 10, 2021, we shut down many of our systems proactively after detecting
5 unusual activity on the network. Upon detection, we immediately took all systems
6 offline and took steps to investigate and determine the nature of the incident. Based
7 on the results of that assessment, there is evidence to suggest an unauthorized third
8 party acceded CMC’s network. A comprehensive investigation was also conducted
9 to identify any instances of sensitive data compromise so that we could contact
10 individuals who may have been affected by this incident.

11 This letter serves to notify you that it is possible the following personal information
12 could have been compromised by an unauthorized third party: first and last name,
13 mailing address, Social Security number, date of birth, demographic information,
14 and medical information maintained by CMC.

15 36. In response to the Data Breach, Defendant stated it “continue[s] to make progress
16 on restoring all systems safely and returning to normal operations.”¹⁴ Furthermore, Defendant
17 acknowledged that its previous cybersecurity policies and procedures were lacking and need
18 improvement: “We have also taken steps to improve our network security to further secure
19 sensitive data and prevent any misuse of patient information.”¹⁵ Defendant claims that it “will
20 continue to work with law enforcement and cybersecurity experts to assess the full scope and
21 nature of the incident, as well as to fix the situation.”¹⁶ The details of the root cause of the Data
22 Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a
23 breach does not occur again have not been shared with Plaintiffs and Class Members, who retain
24 a vested interest in ensuring that their PHI/PII remains protected.¹⁷

25 37. The unencrypted PHI/PII of Plaintiffs and Class Members may end up for sale on

¹⁴ <http://www.communitymedicalcenters.org/News/update-on-recent-network-security-incident-2021> (last visited June 6, 2022).

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

1 the dark web, or simply fall into the hands of companies that will use the detailed PHI/PII for
2 targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized
3 individuals can easily access the PHI/PII of Plaintiffs and Class Members.

4 38. Defendant did not use reasonable security procedures and practices appropriate to
5 the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, such
6 as encrypting the information or deleting it when it is no longer needed, causing the exposure of
7 PHI/PII for many current and former patients.

8 39. As explained by the Federal Bureau of Investigation, “[p]revention is the most
9 effective defense against ransomware and it is critical to take precautions for protection.”¹⁸

10 40. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could
11 and should have implemented, as recommended by the United States Government, the following
12 measures, which, on information and belief, it did not:

- 13 • Implement an awareness and training program. Because end users are targets,
14 employees and individuals should be aware of the threat of ransomware and how it is
delivered.
- 15 • Enable strong spam filters to prevent phishing emails from reaching the end users and
16 authenticate inbound email using technologies like Sender Policy Framework (SPF),
Domain Message Authentication Reporting and Conformance (DMARC), and
DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- 17 • Scan all incoming and outgoing emails to detect threats and filter executable files from
18 reaching end users.
- 19 • Configure firewalls to block access to known malicious IP addresses.
- 20 • Patch operating systems, software, and firmware on devices. Consider using a
centralized patch management system.
- 21 • Set anti-virus and anti-malware programs to conduct regular scans automatically.
- 22 • Manage the use of privileged accounts based on the principle of least privilege: no
23

24 ¹⁸ How to Protect Your Networks from RANSOMWARE, at 3, *available at*:
25 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last
visited June 6, 2022).

1 users should be assigned administrative access unless absolutely needed; and those
2 with a need for administrator accounts should only use them when necessary.

- 3 • Configure access controls—including file, directory, and network share permissions—
4 with least privilege in mind. If a user only needs to read specific files, the user should
5 not have write access to those files, directories, or shares.
- 6 • Disable macro scripts from office files transmitted via email. Consider using Office
7 Viewer software to open Microsoft Office files transmitted via email instead of full
8 office suite applications.
- 9 • Implement Software Restriction Policies (SRP) or other controls to prevent programs
10 from executing from common ransomware locations, such as temporary folders
11 supporting popular Internet browsers or compression/decompression programs,
12 including the AppData/LocalAppData folder.
- 13 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 14 • Use application whitelisting, which only allows systems to execute programs known
15 and permitted by security policy.
- 16 • Execute operating system environments or specific programs in a virtualized
17 environment.
- 18 • Categorize data based on organizational value and implement physical and logical
19 separation of networks and data for different organizational units.¹⁹

20 41. To prevent and detect cyber-attacks Defendant could and should have implemented,
21 as recommended by the United States Cybersecurity & Infrastructure Security Agency, the
22 following measures:

- 23 • **Update and patch your computer.** Ensure your applications and operating systems
24 (OSs) have been updated with the latest patches. Vulnerable applications and OSs are
25 the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when
clicking directly on links in emails, even if the sender appears to be someone you
know. Attempt to independently verify website addresses (e.g., contact your
organization's helpdesk, search the internet for the sender organization's website or
the topic mentioned in the email). Pay attention to the website addresses you click on,
as well as those you enter yourself. Malicious website addresses often appear almost
identical to legitimate sites, often using a slight variation in spelling or a different
domain (e.g., .com instead of .net)....

¹⁹ *Id.* at 3-4.

- 1 • **Open email attachments with caution.** Be wary of opening email attachments, even
2 from senders you think you know, particularly when attachments are compressed files
or ZIP files.
- 3 • **Keep your personal information safe.** Check a website’s security to ensure the
4 information you submit is encrypted before you provide it....
- 5 • **Verify email senders.** If you are unsure whether or not an email is legitimate, try to
6 verify the email’s legitimacy by contacting the sender directly. Do not click on any
links in the email. If possible, use a previous (legitimate) email to ensure the contact
information you have for the sender is authentic before you contact them.
- 7 • **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to
8 date on ransomware techniques. You can find information about known phishing
attacks on the Anti-Phishing Working Group website. You may also want to sign up
9 for CISA product notifications, which will alert you when a new Alert, Analysis
Report, Bulletin, Current Activity, or Tip has been published.
- 10 • **Use and maintain preventative software programs.** Install antivirus software,
11 firewalls, and email filters—and keep them updated—to reduce malicious network
traffic....²⁰

12 42. To prevent and detect cyber-attacks or ransomware attacks Defendant could and
13 should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team,
14 the following measures:

15 **Secure internet-facing assets**

- 16 - Apply latest security updates
- 17 - Use threat and vulnerability management
- 18 - Perform regular audit; remove privileged credentials;

19 **Thoroughly investigate and remediate alerts**

- 20 - Prioritize and treat commodity malware infections as potential full
21 compromise;

22 **Include IT Pros in security discussions**

- 23 - Ensure collaboration among [security operations], [security admins], and
24 [information technology] admins to configure servers and other endpoints
25 securely;

²⁰ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited June 6, 2022).

1 **Build credential hygiene**

- 2 - Use [multifactor authentication] or [network level authentication] and use
3 strong, randomized, just-in-time local admin passwords;

4 **Apply principle of least-privilege**

- 5 - Monitor for adversarial activities
6 - Hunt for brute force attempts
7 - Monitor for cleanup of Event Logs
8 - Analyze logon events;

9 **Harden infrastructure**

- 10 - Use Windows Defender Firewall
11 - Enable tamper protection
12 - Enable cloud-delivered protection
13 - Turn on attack surface reduction rules and [Antimalware Scan
14 Interface] for Office [Visual Basic for Applications].²¹

15 43. Given that Defendant was storing the PHI/PII of its and/or other healthcare
16 providers' current and former patients, Defendant could and should have implemented all of the
17 above measures to prevent and detect ransomware attacks.

18 44. The occurrence of the Data Breach indicates that Defendant failed to adequately
19 implement one or more of the above measures to prevent ransomware attacks, resulting in the Data
20 Breach and the exposure of the PHI/PII of an undisclosed number of current and former patients,
21 including Plaintiffs and Class Members.

22 ***Defendant Acquires, Collects, and Stores the PHI & PII of Plaintiffs and Class Members***

23 45. Defendant has historically acquired, collected, and stored the PHI/PII of Plaintiffs
24 and Class Members.

25 46. As part of receiving treatment from Defendant, Plaintiffs and Class Members, as

²¹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available*
at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited June 7, 2022).

1 patients of Defendant and/or other healthcare providers, are required to give their sensitive and
2 confidential PHI/PII to Defendant. Defendant retains this information.

3 47. According to Defendant’s Privacy Policy, it collects sensitive patient information
4 and is legally obligated to protect such information:

5 When you receive treatment and other health care services from us, we create a
6 record of the services you received. We need this record to provide you with quality
care and to comply with legal requirements.

7 * * * *

8 We are required by law to:
9 make sure that health information that identifies you is kept private in accordance
10 with relevant law.
11 give you notice of our legal duties and privacy practices with respect to your
personal information.
12 follow the terms of the notice that is currently in effect for all your personal health
information.²²

13 48. By permitting the Data Breach to occur, Defendant failed to “make sure that the
14 health information that identifies” Plaintiffs and similarly situated CMC patients “is kept private.”

15 49. By obtaining, collecting, and storing the PHI/PII of Plaintiffs and Class Members,
16 Defendant assumed legal and equitable duties and knew or should have known that it was
17 responsible for protecting the PHI/PII from disclosure.

18 50. Plaintiffs and Class Members have taken reasonable steps to maintain the
19 confidentiality of their PHI/PII and relied on Defendant to keep their PHI/PII confidential and
20 maintained securely, to use this information for business purposes only, and to make only
21 authorized disclosures of this information.

22 51. Defendant could have prevented this Data Breach by properly securing and
23 encrypting the files and file servers containing the PHI/PII of Plaintiffs and Class Members.

24 52. Defendant’s policies on its website include promises and legal obligations to

25 ²² Ex. 1.

1 maintain and protect PHI/PII, demonstrating an understanding of the importance of securing
2 PHI/PII.

3 53. Defendant’s negligence in safeguarding the PHI/PII of Plaintiffs and Class
4 Members is exacerbated by the repeated warnings and alerts directed to protecting and securing
5 sensitive data.

6 54. Despite the prevalence of public announcements of data breach and data security
7 compromises, Defendant failed to take appropriate steps to protect the PHI/PII of Plaintiffs and
8 Class Members from being compromised.

9 55. Defendant assures its patients that it is concerned about PHI/PII security, as shown
10 above in its Privacy Policy.

11 ***Defendant Knew or Should Have Known of the Risk Because the Healthcare Sector Is
12 Particularly Susceptible to Cyber Attacks***

13 56. Defendant knew and understood unprotected or exposed PHI/PII in the custody of
14 healthcare companies, such as Defendant, is valuable and highly sought after by nefarious third
15 parties seeking to illegally monetize that PHI/PII through unauthorized access.

16 57. The healthcare sector reported the second largest number of data breaches among
17 all measured sectors in 2018, with the highest rate of exposure per breach.²³ Indeed, when
18 compromised, healthcare related data is among the most sensitive and personally consequential. A
19 report focusing on healthcare breaches found the “average total cost to resolve an identity theft-
20 related incident . . . came to about \$20,000,” and that victims were often forced to pay out of pocket
21 costs for healthcare they did not receive in order to restore coverage.²⁴ Almost 50 percent of the

22 ²³ See Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, available at:
23 [https://www.idtheftcenter.org/wp-content/uploads/2018/12/2018-November-Data-Breach-
Package.pdf](https://www.idtheftcenter.org/wp-content/uploads/2018/12/2018-November-Data-Breach-Package.pdf) (last visited June 7, 2022).

24 ²⁴ See Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010),
25 available at: <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last
visited June 7, 2022).

1 victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their
2 insurance premiums went up after the event. Forty percent of the customers were never able to
3 resolve their identity theft at all. Data breaches and identity theft have a crippling effect on
4 individuals and detrimentally impacts the economy as a whole.²⁵

5 58. Healthcare related data breaches continue to rapidly increase. According to the 2019
6 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders
7 reported having a significant security incident within the previous 12 months, and most of these
8 known incidents were caused by “bad actors,” such as cybercriminals.²⁶ “Hospitals have emerged
9 as a primary target because they sit on a gold mine of sensitive personally identifiable information
10 (PII) for thousands of patients at any given time. From social security and insurance policies to
11 next of kin and credit cards, no other organization, including credit bureaus, have so much
12 monetizable information stored in their data centers.”²⁷

13 59. As a healthcare provider, Defendant knew, or should have known, the importance
14 of safeguarding PHI/PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable
15 consequences if its data security systems were breached. This includes the significant costs
16 imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to
17 take adequate cybersecurity measures to prevent the Data Breach.

18 ***Value of Personally Identifiable Information***

19 60. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
20
21

22 ²⁵ See *id.*

23 ²⁶ See 2019 HIMSS Cybersecurity Survey, available at:
https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited June 7, 2022).

24 ²⁷ See Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*,
April 4, 2019, available at: <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited June 7, 2022).

1 committed or attempted using the identifying information of another person without authority.”²⁸
2 The FTC describes “identifying information” as “any name or number that may be used, alone or
3 in conjunction with any other information, to identify a specific person,” including, among other
4 things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s
5 license or identification number, alien registration number, government passport number,
6 employer or taxpayer identification number.”²⁹

7 61. The PII of individuals remains of high value to criminals, as evidenced by the prices
8 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
9 credentials. For example, PII can be sold at a price ranging from \$40 to \$200, and bank details
10 have a price range of \$50 to \$200.³⁰ Experian reports that a stolen credit or debit card number can
11 sell for \$5 to \$110 on the dark web.³¹ Criminals can also purchase access to entire company data
12 breaches from \$900 to \$4,500.³²

13 62. Social Security numbers, for example, are among the worst kind of PII to have
14 stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to
15 change. The Social Security Administration stresses that the loss of an individual’s Social Security
16 number, as is the case here, can lead to identity theft and extensive financial fraud:

17 A dishonest person who has your Social Security number can use it to get other
18 personal information about you. Identity thieves can use your number and your
19 good credit to apply for more credit in your name. Then, they use the credit cards
and don’t pay the bills, it damages your credit. You may not find out that someone

20 ²⁸ 17 C.F.R. § 248.201 (2013).

21 ²⁹ *Id.*

22 ³⁰ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends,
Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited June 7, 2022).

23 ³¹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian,
Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited June 7, 2022).

24 ³² *In the Dark*, VPNOverview, 2019, available at:
25 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited June 7, 2022).

1 is using your number until you're turned down for credit, or you begin to get calls
2 from unknown creditors demanding payment for items you never bought. Someone
3 illegally using your Social Security number and assuming your identity can cause
4 a lot of problems.³³

5 63. What is more, it is no easy task to change or cancel a stolen Social Security number.
6 An individual cannot obtain a new Social Security number without significant paperwork and
7 evidence of actual misuse. In other words, preventive action to defend against the possibility of
8 misuse of a Social Security number is not permitted; an individual must show evidence of actual,
9 ongoing fraud activity to obtain a new number.

10 64. Even then, a new Social Security number may not be effective. According to Julie
11 Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link
12 the new number very quickly to the old number, so all of that old bad information is quickly
13 inherited into the new Social Security number.”³⁴

14 65. Based on the foregoing, the information compromised in the Data Breach is
15 significantly more valuable than the loss of, for example, credit card information in a retailer data
16 breach because, there, victims can cancel or close credit and debit card accounts. The information
17 compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to
18 change—Social Security number, driver’s license number, name, and date of birth.

19 66. This data demands a much higher price on the black market. Martin Walter, senior
20 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
21 personally identifiable information and Social Security numbers are worth more than 10x in price

22 ³³ Social Security Administration, *Identity Theft and Your Social Security Number*, available
23 at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited June 7, 2022).

24 ³⁴ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*,
25 NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited June 7, 2022).

1 on the black market.”³⁵

2 67. Among other forms of fraud, identity thieves may obtain driver’s licenses,
3 government benefits, medical services, and housing or even give false information to police.

4 68. The fraudulent activity resulting from the Data Breach may not come to light for
5 years.

6 69. There may be a time lag between when harm occurs versus when it is discovered,
7 and also between when PII is stolen and when it is used. According to the U.S. Government
8 Accountability Office (“GAO”), which conducted a study regarding data breaches:

9 [L]aw enforcement officials told us that in some cases, stolen data may be held for
10 up to a year or more before being used to commit identity theft. Further, once stolen
11 data have been sold or posted on the Web, fraudulent use of that information may
continue for years. As a result, studies that attempt to measure the harm resulting
from data breaches cannot necessarily rule out all future harm.³⁶

12 70. At all relevant times, Defendant knew, or reasonably should have known, of the
13 importance of safeguarding the PHI/PII of Plaintiffs and Class Members, including Social Security
14 numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant’s
15 data security system was breached, including, specifically, the significant costs that would be
16 imposed on Plaintiffs and Class Members as a result of a breach.

17 71. Plaintiffs and Class Members now face years of constant surveillance of their
18 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
19 continue to incur such damages in addition to any fraudulent use of their PHI/PII.

20 72. Defendant was, or should have been, fully aware of the unique type and the
21

22 ³⁵ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit*
23 *Card Numbers*, IT World, (Feb. 6, 2015), available at:
<https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited June 7, 2022).

24 ³⁶ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
25 <https://www.gao.gov/assets/gao-07-737.pdf> (last visited June 7, 2022).

1 significant volume of data on Defendant’s server(s), amounting to potentially thousands of
2 individuals’ detailed PHI/PII and, thus, the significant number of individuals who would be
3 harmed by the exposure of the unencrypted data.

4 73. In the breach notification letter, Defendant made an offer of 12 months of identity
5 monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it
6 fails to provide for the fact that victims of data breaches and other unauthorized disclosures
7 commonly face multiple years of ongoing identity theft, and medical and financial fraud, and it
8 entirely fails to provide sufficient compensation for the unauthorized release and disclosure of
9 Plaintiffs’ and Class Members’ PHI/PII.

10 74. The injuries to Plaintiffs and Class Members were directly and proximately caused
11 by Defendant’s failure to implement or maintain adequate data security measures for the PHI/PII
12 of Plaintiffs and Class Members.

13 75. The ramifications of Defendant’s failure to keep secure the PHI/PII of Plaintiffs and
14 Class Members are long lasting and severe. Once PHI/PII is stolen, particularly Social Security
15 numbers, fraudulent use of that information and damage to victims may continue for years.

16 ***Plaintiff Daniel Hinds’ Experience***

17 76. Plaintiff Hinds is a victim of the Data Breach.

18 77. Prior to the Data Breach, Defendant was Plaintiff Hinds’ primary care provider. In
19 order to receive medical services from Defendant, Plaintiff Hinds provided Defendant with highly
20 sensitive personal and medical information. As a result, Plaintiff Hinds’ information was among
21 the data accessed by an unauthorized third party in the Data Breach.

22 78. Plaintiff Hinds received—and was a “consumer” for purposes of obtaining—
23 medical services from Defendant within the State of California.

24 79. At all times herein relevant, Plaintiff Hinds is and was a member of the Class.

1 99. Plaintiff Dawood stores any documents containing his PHI/PII in a safe and secure
2 location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

3 100. Shortly after October 25, 2021, Plaintiff Dawood received notice from Defendant
4 that his PHI/PII had been improperly accessed and/or obtained by unauthorized third parties. This
5 notice indicated that Plaintiff Dawood's PHI/PII, including first and last name, address, date of
6 birth, Social Security number, demographic information and medical information was
7 compromised as a result of the Data Breach.

8 101. After and as a result of the Data Breach, Plaintiff Dawood has experienced a
9 substantial increase (three or four additional spam calls or emails per day) in suspicious scam
10 phone calls and emails, all of which appear to be placed with the intent to obtain personal
11 information to commit identity theft by way of a social engineering attack.

12 102. As a result of the Data Breach and the subsequent increase in scam calls and emails,
13 Plaintiff Dawood made reasonable efforts to mitigate the impact of the Data Breach, including but
14 not limited to researching the Data Breach and reviewing credit reports and financial account
15 statements more frequently for any indications of actual or attempted identity theft or fraud.
16 Plaintiff Dawood has spent many hours dealing with the Data Breach, valuable time Plaintiff
17 Dawood otherwise would have spent on other activities, including but not limited to work and/or
18 recreation.

19 103. Plaintiff Dawood suffered actual injury from having his PHI/PII compromised as a
20 result of the Data Breach including, but not limited to (a) damage to and diminution in the value
21 of his PHI/PII, a form of property that Defendant obtained from Plaintiff Dawood; (b) violation of
22 his privacy rights; and (c) present, imminent and impending injury arising from the increased risk
23 of identity theft and fraud.

24 104. As a result of the Data Breach, Plaintiff Dawood anticipates spending considerable
25

1 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
2 Breach. As a result of the Data Breach, Plaintiff Dawood is at a present risk and will continue to
3 be at increased risk of identity theft and fraud for years to come.

4 ***Plaintiff Lopez's Experience***

5 105. Plaintiff Lopez was required to provide her PHI/PII to Defendant in connection with
6 her receiving medical treatment from Defendant in the past.

7 106. Plaintiff Lopez typically takes measures to protect her PHI/PII, and is very careful
8 about sharing her PHI/PII. She has never knowingly transmitted unencrypted PII or PHI over the
9 internet or any other unsecured source.

10 107. Plaintiff Lopez stores any documents containing her PHI/PII in a safe and secure
11 location. Moreover, she diligently chooses unique usernames and passwords for her online
12 accounts.

13 108. Shortly after October 25, 2021, Plaintiff Lopez received notice from Defendant
14 that her PHI/PII had been improperly accessed and/or obtained by unauthorized third parties. This
15 notice indicated that Plaintiff Lopez's PHI/PII, including first and last name, address, date of birth,
16 Social Security number, demographic information and medical information was compromised as
17 a result of the Data Breach.

18 109. After and as a result of the Data Breach, Plaintiff Lopez has experienced a
19 substantial increase (twenty additional spam calls or texts per day) in suspicious scam phone calls
20 and texts, all of which appear to be placed with the intent to obtain personal information to commit
21 identity theft by way of a social engineering attack.

22 110. As a result of the Data Breach and the subsequent substantial increase in scam calls
23 and texts, Plaintiff Lopez made reasonable efforts to mitigate the impact of the Data Breach.
24

1 Plaintiff Lopez has spent hours dealing with the Data Breach, valuable time Plaintiff Lopez
2 otherwise would have spent on other activities, including but not limited to work and/or recreation.

3 111. Plaintiff Lopez suffered actual injury from having her PHI/PII compromised as a
4 result of the Data Breach including, but not limited to (a) damage to and diminution in the value
5 of her PHI/PII, a form of property that Defendant obtained from Plaintiff Lopez; (b) violation of
6 her privacy rights; and (c) present, imminent and impending injury arising from the increased risk
7 of identity theft and fraud.

8 112. As a result of the Data Breach, Plaintiff Lopez anticipates spending considerable
9 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
10 Breach. As a result of the Data Breach, Plaintiff Lopez is at a present risk and will continue to be
11 at increased risk of identity theft and fraud for years to come.

12 ***Plaintiff Palermo's Experience***

13 113. Plaintiff Palermo was required to provide his PII to Defendant in connection with
14 receiving medical treatment from Defendant in the past.

15 114. Plaintiff Palermo received a "Notice of Data Breach" letter dated October 25, 2021,
16 on or about that date. The letter notified Plaintiff Palermo that an unauthorized third party could
17 have accessed his full name, mailing address, Social Security number, date of birth, demographic
18 information and medical information.

19 115. As a result of the Data Breach, Plaintiff Palermo spent time dealing with the
20 consequences of the Data Breach, which includes time spent on the telephone verifying the
21 legitimacy of the Data Breach, researching credit monitoring options, signing up for the credit
22 monitoring offered by Defendant, monitoring his medical records for identity/informational theft,
23 and self-monitoring his financial accounts. This time has been lost forever and cannot be
24 recaptured.

1 Breach. As a result of the Data Breach, Plaintiff Palermo is at a present risk and will continue to
2 be at increased risk of identity theft and fraud for years to come.

3 *Plaintiff Miranda's Experience*

4 123. More than 10 years before the Data Breach, Plaintiff Miranda visited one of
5 Defendant's facilities ahead of the birth of her son, which required that Plaintiff Miranda produce
6 her Social Security number, among other personal and medical information, to Defendant.

7 124. Approximately four years before the Data Breach, Plaintiff Miranda last visited one
8 of Defendant's facilities.

9 125. On or around November 1, 2021, Plaintiff Miranda received a Notice of Data
10 Breach from Defendant.

11 126. As a result of the Data Breach, Plaintiff Miranda spent time dealing with the
12 consequences of the Data Breach, which includes time spent on the telephone and sorting through
13 her unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring
14 and identity theft insurance options, attempting to enroll in the credit monitoring and identity theft
15 protection services offered by Defendant, and self-monitoring her accounts. This time has been
16 lost forever and cannot be recaptured.

17 127. Additionally, Plaintiff Miranda is very careful about sharing her PHI/PII. She has
18 never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

19 128. Plaintiff Miranda stores any documents containing her PHI/PII in a safe and secure
20 location. Moreover, she diligently chooses unique usernames and passwords for her few online
21 accounts.

22 129. Plaintiff Miranda suffered actual injury in the form of damages to and diminution
23 in the value of her PHI/PII—a form of intangible property that Plaintiff Miranda entrusted to
24

1 Defendant for the purpose of obtaining healthcare from Defendant, which was actually or
2 potentially compromised in and as a result of the Data Breach.

3 130. Plaintiff Miranda suffered lost time, annoyance, interference, and inconvenience as
4 a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

5 131. Plaintiff Miranda has suffered injury arising from the substantially increased risk of
6 fraud, identity theft, and misuse resulting from her PHI/PII, especially her Social Security number,
7 in combination with her name, being placed in the hands of unauthorized third-parties and possibly
8 criminals.

9 132. Plaintiff Miranda has a continuing interest in ensuring that her PHI/PII, which, upon
10 information and belief, remain backed up in Defendant's possession, is protected and safeguarded
11 from future breaches.

12 **V. CLASS ALLEGATIONS**

13 133. This action is properly maintainable as a class action. Plaintiffs bring this class
14 action on behalf of themselves and on behalf of all others similarly situated pursuant to the Code
15 of Civil Procedure § 382, for the following class defined as:

16 All individuals residing in the United States whose PHI/PII was compromised in
17 the data breach first announced by Defendant on or about October 25, 2021 (the
"Nationwide Class").

18 134. Additionally, Plaintiffs bring this class action on behalf of themselves and on behalf
19 of all others similarly situated pursuant to the Code of Civil Procedure § 382 for the following
20 subclass defined as:

21 All individuals residing in California whose PHI/PII was compromised in the data
22 breach first announced by Defendant on or about October 25, 2021 (the "California
Subclass").

23 135. The Nationwide Class and California Subclass are collectively referred to herein as
24 the "Class" or "Classes."

- 1 f. Whether Defendant adequately and accurately informed Plaintiffs and Class
2 Members that their PHI/PII had been compromised;
- 3 g. Whether Defendant failed to implement and maintain reasonable security procedures
4 and practices appropriate to the nature and scope of the information compromised in
5 the Data Breach;
- 6 h. Whether Defendant adequately addressed and fixed the vulnerabilities which
7 permitted the Data Breach to occur;
- 8 i. Whether Defendant engaged in unfair, unlawful, or deceptive acts or practices by
9 failing to safeguard the PHI/PII of Plaintiffs and Class Members;
- 10 j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory
11 damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- 12 k. Whether Plaintiffs and Class Members are entitled to restitution as a result of
13 Defendant's wrongful conduct; and
- 14 l. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the
15 imminent and currently ongoing harm faced as a result of the Data Breach.

16 140. Typicality: Plaintiffs' claims are typical of those of the other members of the
17 Classes because Plaintiffs, like every other member, was exposed to virtually identical conduct
18 and now suffers from the same violations of the law as other members of the Classes.

19 141. Policies Generally Applicable to the Classes: This class action is also appropriate
20 for certification because Defendant acted or refused to act on grounds generally applicable to the
21 Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards
22 of conduct toward the Class Members and making final injunctive relief appropriate with respect
23 to the Nationwide Class as a whole and to the California Subclass as a whole. Defendant's policies
24 challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these

1 policies hinges on Defendant's conduct with respect to the Classes each as a whole, not on facts
2 or law applicable only to Plaintiffs.

3 142. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests
4 of the Class Members in that they have no disabling conflicts of interest that would be antagonistic
5 to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the
6 Class Members and the infringement of the rights and the damages they have suffered are typical
7 of other Class Members. Plaintiffs have retained counsel experienced in complex class action
8 litigation, and Plaintiffs intend to prosecute this action vigorously.

9 143. Superiority and Manageability: Class litigation is an appropriate method for fair
10 and efficient adjudication of the claims involved. Class action treatment is superior to all other
11 available methods for the fair and efficient adjudication of the controversy alleged herein; it will
12 permit a large number of Class Members to prosecute their common claims in a single forum
13 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and
14 expense that hundreds of individual actions would require. Class action treatment will permit the
15 adjudication of relatively modest claims by certain Class Members, who could not individually
16 afford to litigate a complex claim against a large corporation, like Defendant. Further, even for
17 those Class Members who could afford to litigate such a claim, it would still be economically
18 impractical and impose a burden on the courts.

19 144. The nature of this action and the nature of laws available to Plaintiffs and Class
20 Members make the use of the class action device a particularly efficient and appropriate procedure
21 to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would
22 necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the
23 limited resources of each individual Class Member with superior financial and legal resources; the
24 costs of individual suits could unreasonably consume the amounts that would be recovered; proof

1 of a common course of conduct to which Plaintiffs were exposed is representative of that
2 experienced by the Classes and will establish the right of each Class Member to recover on the
3 causes of action alleged; and individual actions would create a risk of inconsistent results and
4 would be unnecessary and duplicative of this litigation.

5 145. The litigation of the claims brought herein is manageable. Defendant's uniform
6 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
7 Members demonstrates that there would be no significant manageability problems with
8 prosecuting this lawsuit as a class action.

9 146. Adequate notice can be given to Class Members directly using information
10 maintained in Defendant's records.

11 147. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
12 properly secure the PHI/PII of Class Members, Defendant may continue to refuse to provide proper
13 notification to Class Members regarding the Data Breach, and Defendant may continue to act
14 unlawfully as set forth in this Complaint.

15 **FIRST CAUSE OF ACTION**
16 **NEGLIGENCE**
(On Behalf of Plaintiffs and the Nationwide Class)

17 148. Plaintiffs re-allege and incorporate by reference herein all of the allegations
18 contained in paragraphs 1 through 147.

19 149. As a condition of receiving services from Defendant, Defendant's current and
20 former patients were obligated to provide Defendant with PHI/PII, including, but not limited to,
21 their names, addresses, dates of birth, Social Security numbers, demographic information, and
22 medical information.

23 150. Plaintiffs and the Class entrusted their PHI/PII to Defendant on the premise and
24 with the understanding that Defendant would safeguard their information, use their PHI/PII for

1 business purposes only, and/or not disclose their PHI/PII to unauthorized third parties.

2 151. Defendant has full knowledge of the sensitivity of the PHI/PII and the types of harm
3 that Plaintiffs and the Class could and would suffer if the PHI/PII were wrongfully disclosed.

4 152. Defendant knew or reasonably should have known that the failure to exercise due
5 care in the collecting, storing, and using of the PHI/PII of Plaintiffs and the Class involved an
6 unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the
7 criminal acts of a third party.

8 153. Defendant had a duty to exercise reasonable care in safeguarding, securing, and
9 protecting such information from being compromised, lost, stolen, misused, and/or disclosed to
10 unauthorized parties. This duty includes, among other things, designing, maintaining, and testing
11 Defendant's security protocols to ensure that the PHI/PII of Plaintiffs and the Class in Defendant's
12 possession was adequately secured and protected.

13 154. Defendant also had a duty to exercise appropriate clearinghouse practices to remove
14 former patients' PHI/PII that Defendant was no longer required to retain pursuant to regulations.

15 155. Defendant also had a duty to have procedures in place to detect and prevent the
16 improper access and misuse of the PHI/PII of Plaintiffs and the Class.

17 156. Defendant's duty to use reasonable security measures arose as a result of the special
18 relationship that existed between Defendant on the one hand and Plaintiffs and the Class on the
19 other. That special relationship arose because Plaintiffs and the Class entrusted Defendant with
20 their confidential PHI/PII, a necessary part receiving services from Defendant.

21 157. Defendant was subject to an "independent duty," untethered to any contract
22 between Defendant and Plaintiffs or the Class.

23 158. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the
24 Class were reasonably foreseeable, particularly in light of Defendant's inadequate security

1 practices.

2 159. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate
3 security practices and procedures. Defendant knew or should have known of the inherent risks in
4 collecting and storing the PHI/PII of Plaintiffs and the Class, the critical importance of providing
5 adequate security of that information, and the necessity for encrypting or redacting PHI/PII stored
6 on Defendant's systems.

7 160. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the
8 Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and
9 opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included
10 its decisions to not comply with industry standards for the safekeeping of the PHI/PII of Plaintiffs
11 and the Class, including basic encryption techniques freely available to Defendant.

12 161. Plaintiffs and the Class had no ability to protect their PHI/PII that was in, and
13 possibly remains in, Defendant's possession.

14 162. Defendant was in a position to protect against the harm suffered by Plaintiffs and
15 the Class as a result of the Data Breach.

16 163. Defendant had and continues to have a duty to adequately disclose that the PHI/PII
17 of Plaintiffs and the Class within Defendant's possession might have been compromised, how it
18 was compromised, and precisely the types of data that were compromised and when. Such notice
19 was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any
20 identity theft and the fraudulent use of their PHI/PII by third parties.

21 164. Defendant had a duty to employ proper procedures to prevent the unauthorized
22 dissemination of the PHI/PII of Plaintiffs and the Class.

23 165. Defendant has admitted that the PHI/PII of Plaintiffs and the Class was wrongfully
24 lost and disclosed to unauthorized third persons as a result of the Data Breach.

1 166. Defendant, through its actions and/or omissions, unlawfully breached its duties to
2 Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in
3 protecting and safeguarding the PHI/PII of Plaintiffs and the Class during the time the PHI/PII was
4 within Defendant's possession or control.

5 167. Defendant improperly and inadequately safeguarded the PHI/PII of Plaintiffs and
6 the Class in deviation of standard industry rules, regulations, and practices at the time of the Data
7 Breach.

8 168. Defendant failed to heed industry warnings and alerts to provide adequate
9 safeguards to protect the PHI/PII of Plaintiffs and the Class in the face of increased risk of theft.

10 169. Defendant, through its actions and/or omissions, unlawfully breached its duty to
11 Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent
12 dissemination of its current and former patients' PHI/PII.

13 170. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and
14 the Class, the PHI/PII of Plaintiffs and the Class would not have been compromised.

15 171. There is a close causal connection between Defendant's failure to implement
16 security measures to protect the PHI/PII of Plaintiffs and the Class and the present harm, or risk
17 of imminent harm, suffered by Plaintiffs and the Class. The PHI/PII of Plaintiffs and the Class was
18 lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in
19 safeguarding such PHI/PII by adopting, implementing, and maintaining appropriate security
20 measures.

21 172. Defendant violated the CMIA, as alleged herein. Defendant's violation of the
22 CMIA constitutes negligence *per se*.

23 173. Plaintiffs and the Class are within the class of persons that the CMIA was intended
24 to protect, and the harm that occurred as a result of the Data Breach is the type of harm the CMIA

1 was intended to guard against.

2 174. As a direct and proximate result of Defendant’s negligence and negligence *per se*,
3 Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual
4 identity theft; (ii) the loss of the opportunity of how their PHI/PII is used; (iii) the compromise,
5 publication, and/or theft of their PHI/PII; (iv) out-of-pocket expenses associated with the
6 prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their
7 PHI/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity
8 addressing and attempting to mitigate the actual present and future consequences of the Data
9 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and
10 recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit
11 reports; (vii) the continued risk to their PHI/PII, which remains in Defendant’s possession and is
12 subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and
13 adequate measures to protect the PHI/PII of Plaintiffs and the Class; and (viii) costs in terms of
14 time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of
15 the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs
16 and the Class.

17 175. As a direct and proximate result of Defendant’s negligence and negligence *per se*,
18 Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm,
19 including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and
20 non-economic losses.

21 176. Additionally, as a direct and proximate result of Defendant’s negligence and
22 negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of
23 exposure of their PHI/PII, which remain in Defendant’s possession and is subject to further
24

1 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
2 measures to protect the PHI/PII in its continued possession.

3 177. Plaintiffs and Class Members are therefore entitled to damages, including
4 restitution and unjust enrichment, declaratory and injunctive relief, and attorney fees, costs, and
5 expenses.

6 **SECOND CAUSE OF ACTION**
7 **BREACH OF IMPLIED CONTRACT**
8 **(On Behalf of Plaintiffs and the Nationwide Class)**

9 178. Plaintiffs re-allege and incorporate by reference herein all of the allegations
10 contained in paragraphs 1 through 147.

11 179. Defendant required Plaintiffs and the Class to provide their PHI/PII, including
12 names, addresses, Social Security numbers, driver's license numbers and medical history
13 information, as a condition of receiving medical services as a patient.

14 180. As a condition of receiving services from Defendant, Plaintiffs and the Class
15 provided their PHI/PII. In so doing, Plaintiffs and the Class entered into implied contracts with
16 Defendant by which Defendant agreed to safeguard and protect such information, to keep such
17 information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if
18 their data had been breached and compromised or stolen.

19 181. Plaintiffs and the Class fully performed their obligations under the implied contracts
20 with Defendant.

21 182. Defendant breached the implied contracts it made with Plaintiffs and the Class by
22 failing to safeguard and protect their PHI/PII, and by failing to provide accurate notice to them
23 that PHI/PII was compromised as a result of the Data Breach.

24 183. As a direct and proximate result of Defendant's above-described breach of implied
25 contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent,

1 and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and
2 economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and
3 economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the
4 compromised data on the dark web; expenses and/or time spent on credit monitoring and identity
5 theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;
6 expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work
7 time; and other economic and non-economic harm.

8 **THIRD CAUSE OF ACTION**
9 **BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING**
10 **(On Behalf of Plaintiffs and the Nationwide Class)**

11 184. Plaintiffs re-allege and incorporate by reference herein all of the allegations
12 contained in paragraphs 1 through 147.

13 185. Every contract in the State of California has an implied covenant of good faith and
14 fair dealing. This implied covenant is an independent duty and may be breached even when there
15 is no breach of a contract's actual and/or express terms.

16 186. Plaintiffs and Class Members have complied with and performed all conditions of
17 their contracts with Defendant.

18 187. Defendant breached the implied covenant of good faith and fair dealing by failing
19 to maintain adequate computer systems and data security practices to safeguard PHI/PII and
20 financial information and continued acceptance of PHI/PII and financial information and storage
21 of other personal information after Defendant knew, or should have known, of the security
22 vulnerabilities of the systems that were exploited in the Data Breach.

23 188. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and
24 Class Members the full benefit of their bargains as originally intended by the parties, thereby
25 causing them injury in an amount to be determined at trial.

1
2 **FOURTH CAUSE OF ACTION**
3 **INVASION OF PRIVACY**
4 **(On Behalf of Plaintiffs and the Class)**

5 189. Plaintiffs re-allege and incorporate by reference herein all of the allegations
6 contained in paragraphs 1 through 147.

7 190. Plaintiffs and the Class had a legitimate expectation of privacy to their PHI/PII and
8 were entitled to the protection of this information against disclosure to unauthorized third parties.

9 191. Defendant owed a duty to its current and former patients, including Plaintiffs and
10 the Class, to keep their PHI/PII contained as a part thereof confidential.

11 192. Defendant failed to protect and released to unknown and unauthorized third parties
12 the PHI/PII of Plaintiffs and the Class.

13 193. Defendant allowed unauthorized and unknown third parties access to and
14 examination of the PHI/PII of Plaintiffs and the Class by way of Defendant's failure to protect the
15 PHI/PII.

16 194. The unauthorized release to, custody of, and examination by unauthorized third
17 parties of the PHI/PII of Plaintiffs and the Class is highly offensive to a reasonable person.

18 195. The intrusion was into a place or thing, which was private and is entitled to be
19 private. Plaintiffs and the Class disclosed their PHI/PII to Defendant as part of the current and
20 former patients' treatment with Defendant, but privately with an intention that the PHI/PII would
21 be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class
22 were reasonable in their belief that such information would be kept private and would not be
23 disclosed without their authorization.

24 196. The Data Breach at the hands of Defendant constitutes an intentional interference
25 with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their persons or as to

1 their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

2 197. Defendant acted with a knowing state of mind when it permitted the Data Breach
3 to occur because it had actual knowledge that its information security practices were inadequate
4 and insufficient.

5 198. Because Defendant acted with this knowing state of mind, it had notice and knew
6 the inadequate and insufficient information security practices would cause injury and harm to
7 Plaintiffs and the Class.

8 199. As a proximate result of the above acts and omissions of Defendant, the PHI/PII of
9 Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiffs and
10 the Class to suffer damages.

11 200. Unless and until enjoined and restrained by order of this Court, Defendant's
12 wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in
13 that the PHI/PII maintained by Defendant can be viewed, distributed, and used by unauthorized
14 persons for years to come. Plaintiffs and the Class have no adequate remedy at law for the injuries
15 in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the
16 Class.

17 **FIFTH CAUSE OF ACTION**
18 **UNJUST ENRICHMENT**
19 **(On Behalf of Plaintiffs and the Nationwide Class)**

20 201. Plaintiffs re-allege and incorporate by reference herein all of the allegations
21 contained in paragraphs 1 through 147.

22 202. Defendant benefited from receiving Plaintiffs' and Class Members' PHI/PII by its
23 ability to retain and use that information for its own benefit. Defendant understood this benefit.
24

1 203. Defendant also understood and appreciated that Plaintiffs' and Class Members'
2 PHI/PII was private and confidential, and its value depended upon Defendant maintaining the
3 privacy and confidentiality of that information.

4 204. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the
5 form of purchasing services from Defendant, and in connection thereto, by providing their PHI/PII
6 to Defendant with the understanding that Defendant would pay for the administrative costs of
7 reasonable data privacy and security practices and procedures. Specifically, they were required to
8 provide Defendant with their PHI/PII. In exchange, Plaintiffs and Class Members should have
9 received adequate protection and data security for such PHI/PII held by Defendant.

10 205. Defendant knew Plaintiffs and Class Members conferred a benefit which Defendant
11 accepted. Defendant profited from these transactions and used the PHI/PII of Plaintiffs and Class
12 Members for business purposes.

13 206. Defendant failed to provide reasonable security, safeguards, and protections to the
14 PHI/PII of Plaintiffs and Class Members.

15 207. Under the principles of equity and good conscience, Defendant should not be
16 permitted to retain money belonging to Plaintiffs and Class Members, because Defendant failed to
17 implement appropriate data management and security measures mandated by industry standards.

18 208. Defendant wrongfully accepted and retained these benefits to the detriment of
19 Plaintiffs and Class Members.

20 209. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was
21 unjust.

22 210. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the
23 Class Members are entitled to restitution and disgorgement of all profits, benefits, and other
24 compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

1
2
3
4

SIXTH CAUSE OF ACTION
VIOLATIONS OF THE CALIFORNIA CONFIDENTIALITY
OF MEDICAL INFORMATION ACT (CMIA)
Cal. Civ. Code § 56, et seq.
(On Behalf of Plaintiffs and the Nationwide Class or, alternatively,
on behalf of the California Subclass)

5 211. Plaintiffs re-allege and incorporate by reference herein all of the allegations
6 contained in paragraphs 1 through 147.

7 212. The short title of the CMIA, Civil Code §§ 56, *et seq.*, states, “The Legislature
8 hereby finds and declares that persons receiving health care services have a right to expect that the
9 confidentiality of individual identifiable medical information derived by health service providers
10 be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for
11 the confidentiality of individually identifiable medical information, while permitting certain
12 reasonable and limited uses of that information.”

13 213. At all relevant times, Defendant created, maintained, preserved, and stored records
14 on its network computer systems of the care, services and products it provided to Plaintiffs and
15 California Subclass Members, including their names, mailing addresses, dates of birth, Social
16 Security numbers, demographic information and medical information (all of which constitutes
17 medical information, as that term is defined and set forth in the CMIA). Plaintiffs and other
18 California Subclass Members and other providers of health care provided this PHI to Defendant.
19 As a result, at all times relevant, Defendant was and is a “provider of health care” within the
20 meaning of Civil Code § 56.05(m).

21 214. At all times relevant, pursuant to Civil Code § 56.06(a), Defendant, as businesses
22 that created, maintained, preserved, and stored records of the care and products and services it
23 and/or other providers of health care, pharmaceutical companies, and contractors as defined by the
24 CMIA provided to Plaintiffs and the California Subclass. These records included their names,

1 Social Security numbers, dates of birth, demographic information and medical information.
2 Defendant is and was, at all times relevant, organized for the purpose of maintaining medical
3 information, within the meaning of Civil Code § 56.05(j), in order to make the information
4 available to an individual or to a provider of health care at the request of the individual or a provider
5 of health care for purposes of allowing the individual to manage his or her information or for the
6 diagnosis and treatment of the individual. Defendant is therefore deemed to be a provider of health
7 care within the meaning of the CMIA.

8 215. Alternatively, at all times relevant, pursuant to Civil Code § 56.05(d), Defendant,
9 as an entity that is a medical group, independent practice association, pharmaceutical benefits
10 manager, or a medical service organization and is not a health care service plan or provider of
11 health care, is and was a “contractor” under Civil Code § 56.05(d).

12 216. Alternatively, at all times relevant, pursuant to Civil Code § 56.13, Defendant is
13 and was a recipient of medical information pursuant to an authorization as provided by the CMIA
14 or pursuant to the provisions of subdivision (c) of Civil Code § 56.10 and was prohibited from
15 further disclosing that medical information except in accordance with a new authorization that
16 meets the requirements of Section 56.11, or as specifically required or permitted by other
17 provisions of the CMIA or by law.

18 217. Alternatively, at all times relevant, pursuant to Civil Code § 56.245, Defendant is
19 and was a recipient of medical information pursuant to an authorization as provided by this chapter,
20 and was prohibited from further disclosing such medical information unless in accordance with a
21 new authorization that meets the requirements of Section 56.21, or as specifically required or
22 permitted by other provisions of the Act or by law.

23 218. Additionally, at all times relevant, pursuant to Civil Code § 56.26(a), Defendant is
24 and was an entity engaged in the business of furnishing administrative services to programs that
25

1 provide payment for health care services, and was prohibited from knowingly using, disclosing or
2 permitting its employees or agents to use or disclose medical information possessed in connection
3 with performing administrative functions for a program, except as reasonably necessary in
4 connection with the administration or maintenance of the program, or as required by law, or with
5 an authorization.

6 219. As a provider of health care, a contractor, and/or other authorized recipient of
7 medical information as defined by Civil Code § 56.05(j), Defendant is required by the CMIA to
8 ensure that medical information regarding patients is not disclosed or disseminated or released
9 without patients' authorization, and to protect and preserve the confidentiality of the medical
10 information regarding a patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and
11 56.36.

12 220. As provider of health care, a contractor, and/or other authorized recipient of medical
13 information as defined by Civil Code § 56.05(j), Defendant is required by the CMIA not to disclose
14 medical information regarding a patient without first obtaining an authorization³⁷ under Civil Code
15 §§ 56.10, 56.13, 56.245 and 56.26.

16
17 ³⁷ An "authorization" is defined under the CMIA as obtaining permission in accordance with
18 Civil Code § 56.11. Under Civil Code § 56.11, an authorization for the release of medical
information is valid only if it:

19 (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point
type.

20 (b) Is clearly separate from any other language present on the same page and is executed
by a signature which serves no other purpose than to execute the authorization.

21 (c) Is signed and dated by one of the following:

22 (1) The patient. A patient who is a minor may only sign an authorization for the
23 release of medical information obtained by a provider of health care, health care
service plan, pharmaceutical company, or contractor in the course of furnishing
services to which the minor could lawfully have consented under Part 1
(commencing with Section 25) or Part 2.7 (commencing with Section 60).

24 (2) The legal representative of the patient, if the patient is a minor or an
25 incompetent. However, authorization may not be given under this subdivision for
the disclosure of medical information obtained by the provider of health care, health

1 221. As a provider of health care, a contractor, and/or other authorized recipient of
2 personal and confidential medical information, Defendant is required by the CMIA to create,
3 maintain, preserve, and store medical records in a manner that preserves the confidentiality of the
4 information contained therein under Civil Code § 56.101(a).

5 222. At all relevant times, as a provider of healthcare a contractor, and/or other
6 authorized recipient of personal and confidential medical information within the meaning of the
7 CMIA, Defendant maintains medical information as defined by Civil Code § 56.05(j) of the
8 Plaintiff and California Subclass.

9 223. Plaintiffs and the Nationwide Class or, alternatively, the California Subclass, are
10 patients within the meaning of Civil Code § 56.05(k).

11 224. Plaintiffs and the Nationwide Class or, alternatively, the California Subclass
12 provided their medical information as defined by Civil Code § 56.05(j) to Defendant or their
13

14 care service plan, pharmaceutical company, or contractor in the course of furnishing
15 services to which a minor patient could lawfully have consented under Part 1
16 (commencing with Section 25) or Part 2.7 (commencing with Section 60).

17 (3) The spouse of the patient or the person financially responsible for the patient,
18 where the medical information is being sought for the sole purpose of processing
19 an application for health insurance or for enrollment in a nonprofit hospital plan, a
20 health care service plan, or an employee benefit plan, and where the patient is to be
21 an enrolled spouse or dependent under the policy or plan.

22 (4) The beneficiary or personal representative of a deceased patient.

23 (d) States the specific uses and limitations on the types of medical information to be
24 disclosed.

25 (e) 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.

(f) States the name or functions of the persons or entities authorized to receive the medical
information.

(g) States the specific uses and limitations on the use of the medical information by the
persons or entities authorized to receive the medical information.

(h) 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.

(i) Advises the person signing the authorization of the right to receive a copy of the
authorization.

1 medical information as defined by Civil Code § 56.05(j) was provided to Defendant by other
2 providers of health care, contractors, and/or other authorized recipients.

3 225. At all relevant times, Defendant collected, stored, managed, and transmitted
4 Plaintiffs' and the Nationwide Class and/or California Subclass's medical information as defined
5 by Civil Code § 56.05(j).

6 226. Section 56.10(a) of the Civil Code provides that “[a] provider of health care, health
7 care service plan, or contractor shall not disclose medical information regarding a patient of the
8 provider of health care or an enrollee or subscriber of a health care service plan without first
9 obtaining an authorization.”

10 227. As a result of the Data Breach, Defendant has released, disclosed, and/or negligently
11 allowed third parties to access and view Plaintiffs' and the Nationwide Class and/or California
12 Subclass' medical information as defined by Civil Code § 56.05(j) without their written
13 authorization as required by the provisions of Civil Code §§ 56, *et seq.* Further, Defendant admits
14 Plaintiffs' and the Nationwide Class and/or California Subclass's names, Social Security numbers,
15 driver's license numbers, dates of birth, demographic information and medical information “on
16 our network appears to have been acquired by an unauthorized third party.”

17 228. The unauthorized third party who committed the Data Breach obtained Plaintiffs'
18 and Nationwide Class and/or California Subclass's medical information as defined by Civil Code
19 § 56.05(j), accessed it, viewed it, and now has it available to them to sell to other bad actors or
20 otherwise misuse.

21 229. As a further result of the Data Breach, the confidential nature of the Plaintiffs' and
22 Nationwide Class or, in the alternative, the California Subclass's medical information as defined
23 by Civil Code § 56.05(j) was breached due to Defendant's negligence or affirmative decisions
24 negligent creation, maintenance, preservation, and/or storage Plaintiffs' and the Nationwide Class

1 or, in the alternative, the California Subclass's medical information as defined by Civil Code §
2 56.05(j) in a manner that did not preserve the confidentiality of the information, and negligently
3 failed to protect and preserve confidentiality of electronic medical information of Plaintiffs and
4 the Class in its possession against disclosure and/or release, including but not limited to, by failing
5 to conduct and require adequate employee education and training, failing to adequately review &
6 revise information security, failing to have adequate information security, not to follow industry
7 best practices, enhance or upgrade security, and failing to have adequate privacy policies and
8 procedures in place, as required by the CMIA, under Civil Code §§ 56.06(d), 56.10(a), 56.13,
9 56.245, 56.26(a), 56.101(a), 56.101(b)(1)(A), and 56.36(e)(2)(E). By such conduct, Defendant
10 allowed at least one unauthorized third party to access and view Plaintiffs' and Nationwide Class
11 or, in the alternative, the California Subclass's medical information as defined by Civil Code
12 § 56.05(j).

13 230. Defendant's release and/or disclosure of medical information regarding Plaintiffs
14 and the Nationwide Class or, in the alternative, the California Subclass constitutes a violation of
15 Civil Code §§ 56.06, 56.10, 56.11, 56.13, 56.26, 56.36, 56.101 and 56.245.

16 231. As a direct and proximate result of Defendant's wrongful actions, inaction,
17 omissions, and want of ordinary care, Plaintiffs' and the Nationwide Class' or, in the alternative,
18 the California Subclass's medical information as defined by Civil Code § 56.05(j) was disclosed
19 without written authorization.

20 232. By disclosing Plaintiffs' and the Nationwide Class' and/or California Subclass'
21 medical information as defined by Civil Code § 56.05(j) without their written authorization,
22 Defendant violated the CMIA and its legal duty to protect the confidentiality of such information.

1 233. Defendant also violated sections 56.06(e) and 56.101(a) of the CMIA, which
2 prohibit the negligent release of Plaintiffs’ and the Nationwide Class and/or California Subclass’
3 medical information as defined by Civil Code § 56.05(j).

4 234. As a direct and proximate result of Defendant’s wrongful actions, inaction,
5 omissions, and want of ordinary care that directly and proximately caused the Data Breach,
6 Plaintiffs’ and the Nationwide Class’ and/or California Subclass’ medical information as defined
7 by Civil Code § 56.05(j) was viewed by, released to, and disclosed to third parties without
8 Plaintiffs’ and the Nationwide Class’ and/or California Subclass’ written authorization and
9 Plaintiffs and the Nationwide Class or, in the alternative, California Subclass are entitled to recover
10 “against any person or entity who has negligently released confidential information or records
11 concerning him or her in violation of this part, for either or both of the following: (1) ... nominal
12 damages of one thousand dollars (\$1,000). In order to recover under this paragraph, it shall not be
13 necessary that the plaintiff suffered or was threatened with actual damages[; and] (2) The amount
14 of actual damages, if any, sustained by the patient.”

15 235. As a direct and proximate result of Defendant’s above-described wrongful actions,
16 inaction, omissions, and want of ordinary care that directly and proximately caused the Data
17 Breach and its violations of the CMIA, Plaintiffs and the Nationwide Class or, in the alternative,
18 the California Subclass are entitled to and hereby seek: (i) actual damages suffered, according to
19 proof, for each violation under Civil Code § 56.36(b)(2); (ii) nominal damages of \$1,000 for each
20 violation under Civil Code §56.36(b)(1); (iii) punitive damages under Civil Code § 56.35; and (iv)
21 attorneys’ fees, litigation expenses, and court costs under Civil Code § 56.35.

22 ///

23 ///

24 ///

- c. Failure to timely and accurately disclose the Data Breach to Plaintiffs and Class Members;
- d. Continued acceptance of PHI/PII and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and
- e. Continued acceptance of PHI/PII and storage of other personal information after Defendant knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

242. Plaintiffs and Class Members suffered injury in fact and lost money or property as the result of Defendant’s unlawful business practices. In addition, Plaintiffs’ and Class Members’ PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

243. Defendant engaged in unfair business practices under the “balancing test.” The harm caused by Defendant’s actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant’s failure to follow basic data security protocols and failure to disclose inadequacies of Defendant’s data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and Class Members, directly causing the harms alleged below.

244. Defendant engaged in unfair business practices under the “tethering test.” Defendant’s actions and omissions, as described in detail above, violated fundamental public

1 complained of herein pertaining to the misuse and/or disclosure of the PHI/PII of
2 Plaintiffs and Class Members, and from refusing to issue complete and accurate
3 disclosures to Plaintiffs and Class Members;

4 C. Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and
5 other equitable relief as is necessary to protect the interests of Plaintiffs and Class
6 Members, including but not limited to an order:

7 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
8 described herein;

9 ii. requiring Defendant to protect, including through encryption, all data collected
10 through the course of its business in accordance with all applicable regulations,
11 industry standards, and federal, state or local laws;

12 iii. requiring Defendant to delete, destroy, and purge the PHI/PII of Plaintiffs and
13 Class Members unless Defendant can provide to the Court reasonable
14 justification for the retention and use of such information when weighed against
15 the privacy interests of Plaintiffs and Class Members;

16 iv. requiring Defendant to implement and maintain a comprehensive Information
17 Security Program designed to protect the confidentiality and integrity of the
18 PHI/PII of Plaintiffs and Class Members;

19 v. prohibiting Defendant from maintaining the PHI/PII of Plaintiffs and Class
20 Members on a cloud-based database;

21 vi. requiring Defendant to engage independent third-party security
22 auditors/penetration testers as well as internal security personnel to conduct
23 testing, including simulated attacks, penetration tests, and audits on
24 Defendant's systems on a periodic basis, and ordering Defendant to promptly

- 1 correct any problems or issues detected by such third-party security auditors;
- 2 vii. requiring Defendant to engage independent third-party security auditors and
- 3 internal personnel to run automated security monitoring;
- 4 viii. requiring Defendant to audit, test, and train its security personnel regarding any
- 5 new or modified procedures;
- 6 ix. requiring Defendant to segment data by, among other things, creating firewalls
- 7 and access controls so that if one area of Defendant's network is compromised,
- 8 hackers cannot gain access to other portions of Defendant's systems;
- 9 x. requiring Defendant to conduct regular database scanning and securing checks;
- 10 xi. requiring Defendant to establish an information security training program that
- 11 includes at least annual information security training for all employees, with
- 12 additional training to be provided as appropriate based upon the employees'
- 13 respective responsibilities with handling personal identifying information, as
- 14 well as protecting the personal identifying information of Plaintiffs and Class
- 15 Members;
- 16 xii. requiring Defendant to routinely and continually conduct internal training and
- 17 education, and on an annual basis to inform internal security personnel how to
- 18 identify and contain a breach when it occurs and what to do in response to a
- 19 breach;
- 20 xiii. requiring Defendant to implement a system of tests to assess its employees'
- 21 knowledge of the education programs discussed in the preceding
- 22 subparagraphs, as well as randomly and periodically testing employees'
- 23 compliance with Defendant's policies, programs, and systems for protecting
- 24 personal identifying information;

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

DATED: June 8, 2022

Respectfully Submitted,

COLE & VAN NOTE

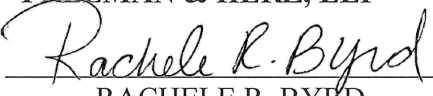
By,


SCOTT EDWARD COLE

Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
Cody Alexander Bolce, Esq. (S.B. #322725)
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
sec@colevannote.com
lvn@colevannote.com
cab@colevannote.com

**WOLF HALDENSTEIN ADLER
FREEMAN & HERZ, LLP**

By,


RACHELE R. BYRD

Betsy C. Manifold (S.B. #182450)
Rachele R. Byrd (S.B. #190634)
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4559
Facsimile: (619) 234-4599
manifold@whafh.com
byrd@whafh.com

*Co-Lead Counsel for Plaintiffs and the
Proposed Class*

Terence R. Coates (*pro hac vice forthcoming*)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 665-0204
Facsimile: (513) 665-0219
tcoates@msdlegal.com

M. Anderson Berry (262879)
Gregory Haroutunian (330263)
CLAYEO C. ARNOLD,

1 **A PROFESSIONAL LAW CORP.**

2 865 Howe Avenue
3 Sacramento, CA 95825
4 Tel: 916.239.4778
5 Fax: 916.924.1829
6 aberry@justice4you.com

7 Gary M. Klinger
8 **MILBERG COLEMAN BRYSON**
9 **PHILLIPS GROSSMAN, PLLC**
10 227 W. Monroe Street, Suite 2100
11 Chicago, IL 60606
12 202/429/2290
13 gklinger@milberg.com

14 David K. Lietz
15 **MILBERG COLEMAN BRYSON**
16 **PHILLIPS GROSSMAN, PLLC**
17 5335 Wisconsin Avenue NW, Suite 440
18 Washington, DC 20015-2052
19 866/252/0878
20 202/686/2877 (fax)
21 dlitz@milberg.com

22 Gary E. Mason
23 Danielle L. Perry (292120)
24 **MASON LLP**
25 5101 Wisconsin Avenue, NW, Suite 305
Washington, DC 20016
202/429-2290
gmason@masonllp.com
dperry@masonllp.com

Michael F. Ram (104805)
Marie N. Appel (187483)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: 415-358-6913
Facsimile: 415-358-6293
mram@forthepeople.com
mappel@forthepeople.com

John A. Yanchunis
Ryan D. Maxey
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor

1 Tampa, Florida 33602
2 Telephone: 813-223-5505
3 jyanchunis@ForThePeople.com
4 rmaxey@ForThePeople.com

5 ROBERT AHDOOT (SBN 172098)
6 TINA WOLFSON (SBN 174806)
7 **AHDOOT & WOLFSON, PC**
8 2600 W. Olive Ave. Suite 500
9 Burbank, CA 91505
10 Tel: (310) 474-9111
11 Fax: (310) 474-8585
12 rahdoot@ahdootwolfson.com
13 twolfson@ahdootwolfson.com

14 BEN BARNOW
15 ANTHONY L. PARKHILL
16 **BARNOW AND ASSOCIATES, P.C.**
17 205 West Randolph Street, Ste. 1630
18 Chicago, IL 60606
19 Tel: (312) 621-2000
20 Fax: (312) 641-5504
21 b.barnow@barnowlaw.com
22 aparkhill@barnowlaw.com

23 *Additional Counsel for Plaintiffs*

24 27841v4

EXHIBIT 1

X

| [Login](#) [Search...](#)

June 09,

Privacy Policy

Notice of Privacy Practices Effective Date 4-14-2003

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY.

For More Information, Please Contact Us:

Custodian of Records

Community Medical Centers, Inc.

Mailing Address: PO Box 779; Stockton, CA 95201

Street Address: 701 E. Channel Street; Stockton, CA 95202

(209) 944-4700; FAX (209) 944-4795

E-Mail to: record@communitymedicalcenters.org

Who We Are:

This Notice describes the privacy practices of **Community Medical Centers, Inc. (CMC)** and the privacy practices of:

all of our doctors, nurses, and other health care professionals authorized to enter information about you into your medical chart.

all of our departments.

all of our health center sites:

all of our employees, staff, volunteers and other personnel who work for us or on our behalf.

Our Pledge:

We understand that health information about you and the health care you receive is personal. We are committed to protecting your personal health information. When you receive treatment and other health care services from us, we create a record of the services that you received. We need this record to provide you with quality care and to comply with legal requirements. This notice applies to all of our records about your care, whether they are created by our health care professionals or others working in this office, and tells you about the ways in which we may use and disclose your personal health information. This notice also describes your rights with respect to the health information that we keep about you and the obligations that we have to protect and disclose your health information.

We are required by law to:

make sure that health information that identifies you is kept private in accordance with relevant law.

give you this notice of our legal duties and privacy practices with respect to your personal health information.

follow the terms of the notice that is currently in effect for all of your personal health information.

How We May Use and Disclose Your Health Information:

We may use and disclose your personal health information for these purposes:

For Treatment. We may use health information about you to provide you with health care treatment or services. We may disclose health information about you to the doctors, nurses, technicians and others who are involved in your care. They may work at CMC, at the hospital if you are hospitalized under our supervision, or at another doctor's office, lab, pharmacy or other health care provider to whom we may refer you for treatment, consultation, x-rays, lab tests, prescriptions or other health care service. They may also include doctors and other health care professionals who work at CMC, or

elsewhere, whom we consult about your care. For example, we may consult with a specialist who lends his/her services to CMC about your care or disclose to an emergency room doctor who is treating you for a broken leg that you have diabetes, because diabetes may affect your body's healing process.

For Payment. We may use and disclose health information about you to bill and collect payment from you, your insurance company, including Medi and Medicare, or other third party that may be available to reimburse us for some or all of your health care. We may also disclose health information about you to other health care providers or to your health plan so that they can arrange for payment relating to your care. For example, if you have health insurance, we may need to share information about your office visit with your health plan in order for your health plan to pay us or reimburse you for the visit. We may also tell your health plan about treatment that you need to obtain your health plan's prior approval or to determine whether your plan will cover the treatment.

For Health Care Operations. We may use and disclose health information about you for our day-to-day operations, and may disclose information about you to other health care providers involved in your care or to your health plan for use in their day-to-day operations. These uses and disclosures are necessary to run CMC and to make sure that all of our patients receive quality care, and to assist other providers and health plans in doing so as well. For example, we may use health information to review the services that we provide and to evaluate the performance of our staff in caring for you. We may also combine health information about our patients with health information from other health care providers to decide what additional services CMC should offer, what services are not needed, whether new treatments are effective or to compare how we are doing with others and to see where we can make improvements. We may remove information that identifies you from this set of health information so others may use it to study health care delivery without learning who our patients are.

Appointment Reminders. We may use and disclose health information about you to contact you as a reminder that you have an appointment at CMC.

Health-Related Services and Treatment Alternatives. We may use and disclose health information to tell you about health-related services or recommend treatment options or alternatives that may be of interest to you. Please let us know if you do not wish us to contact you with this information, or if you wish to have us use a different address when sending this information to you.

Fundraising Activities. We may use health information about you to contact you in an effort to raise money for our not-for-profit operations. We may disclose health information about you to a foundation related to CMC so that the foundation may contact you in raising money for CMC. We will not release contact information, such as your name, address and phone number and the dates you received treatment or services from us. Please let us know if you do not want us to contact you for fundraising efforts.

Individuals Involved in Your Care or Payment for Your Care. We may release health information about you to a friend or family member who is involved in your health care or the person who helps pay for your care.

Research. Under certain circumstances, we may use and disclose health information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another for the same condition. Research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of health information, trying to balance the research needs with a patient's need for privacy. Before we use or disclose health information for research, the project will have been approved through this special approval process, although we may disclose health information about you to people preparing to conduct a research project. For example, we may help potential researchers look for patients with specific health needs, so long as the health information they review does not leave our facility. We will almost always ask for your specific permission if the researcher will have access to your name, address, or other information that reveals who you are or will be involved in your care.

Organ and Tissue Donation. If you are an organ donor, we may disclose health information about you to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

As Required By Law. We will disclose health information about you when required to do so by federal, state or local law.

To Avert a Serious Threat to Health or Safety. We may use and disclose health information about you when necessary to prevent a serious threat to health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

Military and Veterans. If you are a member of the armed forces or separated/ discharged from military services, we may release health information about you as required by military command authorities or the Department of Veterans Affairs as may be applicable. We may also release health information about foreign military personnel to the appropriate foreign military authorities.

Workers' Compensation. We may release health information about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public Health Activities. We may disclose health information about you for public health activities. These activities generally include the following:

- to prevent or control disease, injury or disability.*
- to report births and deaths.*
- to report child abuse or neglect.*
- to report reactions to medications or problems with products.*
- to notify people of recalls of products.*
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition.*
- to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.*

Health Oversight Activities. We may disclose health information about you to a health oversight agency for activities authorized by law. These over activities include, for example, audits, investigations, inspections and licensure. These activities are necessary for the government to monitor the health care system, government programs and compliance with civil rights laws.

Lawsuits and Disputes. We may disclose health information about you in response to a court or administrative order. We may also disclose health information about you in response to a subpoena, discovery request or other lawful process that is not accompanied by a court or administrative order but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Law Enforcement. We may release health information about you if asked to do so by a law enforcement official:

in response to a court order, subpoena, warrant, summons or similar process.
to identify or locate a suspect, fugitive, material witness or missing person.
under certain limited circumstances, about the victim of a crime.
about a death we believe may be the result of criminal conduct.
about criminal conduct at CMC.
in emergency circumstances to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

Coroners, Health Examiners and Funeral Directors. We may release health information about our patients to a coroner or health examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release health information to funeral directors if necessary for them to carry out their duties.

National Security and Intelligence Activities. We may release health information about you to authorized federal officials for intelligence, counterintelligence and other national security activities authorized by law.

Protective Services for the President and Others. We may disclose health information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release health information about you to the corrections institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care to protect your health and safety or the health and safety of others, or (3) for the safety and security of the correctional institution.

Your Rights:

You have certain rights with respect to your personal health information. This section of our notice describes your rights and how to exercise them.

Right to Inspect and Copy: You have the right to inspect and copy the personal health information in your medical and billing records, or in any other group of records that we maintain and use to make health care decisions about you. This right does not include the right to inspect and copy psychotherapy notes, although we may, at your request and on payment of the applicable fee, provide you with a summary of these notes.

To inspect and copy your personal health information, you must submit your request in writing to our privacy contact person identified on the first page of this notice. If you request a copy of the information, we may charge a fee for the copying and mailing costs, and for any other costs associated with your request.

We may deny your request to inspect and copy in certain very limited circumstances. If your request is denied, you may request that the denial be reviewed. We will designate a licensed health care professional to review our decision to deny your request. The person conducting the review will be the same person who denied your request. We will comply with the outcome of this review. Certain denials, such as those relating to psychotherapy notes, however, will not be reviewed.

Right to Amend: If you feel that the health information we maintain about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for any information that we maintain about you. To request an amendment, your request must be made in writing, submitted to our privacy contact person identified on the first page of this notice, and must be contained on one piece of paper legibly handwritten or typed. In addition, you must provide a reason that supports your request for an amendment.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

was not created by us, unless the person or organization that created the information is no longer available to make the amendment,
is not part of the health information kept by or for CMC,
is not part of the information which you would be permitted to inspect and copy, or
is accurate and complete.

Any amendment we make to your health information will be disclosed to the health care professionals involved in your care and to others to carry out payment and health care operations, as previously described in this notice.

Right to Receive an Accounting of Disclosures. You have the right to receive an accounting of certain disclosures of your health information that we have made. Any accounting will not include all disclosures that we make. For example, an accounting will not include disclosures:

to carry out treatment, payment and health care operations as previously described in this notice.
pursuant to your written authorization.
to a family member, other relative, or personal friend involved in your care or payment for your care when you have given us permission to do so.
to law enforcement officials.

To request an accounting of disclosures, you must submit your request in writing to our privacy contact person identified on the first page of this notice. Your request must state a time period which may not be more than six (6) years and may not include dates before April 14, 2003. We may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred. We will mail you a list of disclosures in paper form within 30 days of your request, or notify you if we are unable to mail the list within that time period and by what date we can supply the list; this date will not exceed 60 days from the date you made the request.

Right to Request Restrictions. You have the right to request a restriction or limitation on the health information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the health information we disclose about you to someone who is involved in your care or the payment for your care, such as a family member or friend. For example, you may request that we not disclose information about you to a certain doctor or other health care professional, or that we not disclose information to your spouse about certain care that you received.

We are not required to agree to your request for restrictions if it is not feasible for us to comply with your request or if we believe that it will negatively impact our ability to care for you. If we do agree, however, we will comply with your request unless the information is needed to provide emergency treatment. To request a restriction, you must make your request in writing to our privacy contact person identified on the first page of this notice. In your request, you must tell us what information you want to limit and to whom you want the limits to apply.

Right to Receive Confidential Communications. You have the right to request that we communicate with you about health matters in a certain way. For example, you can ask that we only contact you at work or by mail to a specified address.

To request that we communicate with you in a certain way, you must make your request in writing to our privacy contact person identified on the first page of this notice. We will not ask you the reason for your request. Your request must specify how or where you wish to be contacted. We will accommodate all reasonable requests.

Right to a Paper Copy of this Notice. You have the right to receive a paper copy of this notice at any time. To receive a copy, please request it from our privacy contact person identified on the first page of this notice. You may also obtain a copy of this notice at our website, at www.communitymedicalcenters.org.

Changes to this Notice:

We reserve the right to change this notice and to make the changed notice effective for all of the health information that we maintain about you, whether it is information that we previously received about you or information we may receive about you in the future. We will post a copy of our current notice in our facility. Our notice will indicate the effective date on the first page, in the top right-hand corner. We will also give you a copy of our current notice upon request.

Complaints:

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the Department of Health and Human Services. You may file a complaint by mailing, faxing or e-mailing us a written description of your complaint:

Custodian of Records
Community Medical Centers, Inc.
Mailing Address: PO Box 779; Stockton, CA 95201
Street Address: 701 E. Channel St.; Stockton, CA 95202
(209) 944-4700; FAX (209) 944-4795
E-Mail: record@communitymedicalcenters.org

Please describe what happened and give us the dates and names of anyone involved. Please also let us know how to contact you so that we can respond to your complaint. You will not be penalized for filing a complaint.

Other Uses and Disclosures of Your Protected Health Information:

Other uses and disclosures of personal health information not covered by this notice or applicable law will be made only with your written authorization. If you give us your written authorization to use or disclose your personal health information, you may revoke your authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your personal health information for the reasons covered by your written authorization. You understand that we are unable to take back any uses and disclosures that we have already made with your authorization, and that we are required to retain our records of the care that we have provided to you.

EXHIBIT 2



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Community Medical Centers, Inc. ("CMC") is a non-profit community health center serving San Joaquin, Solano, and Yolo counties in Northern California. We are writing to let you know of an incident that may have exposed some of your personally identifiable and protected health information and provide you with resources you can use to help protect your information.

What Happened and What Information Was Involved:

On October 10, 2021, we shut down many of our systems proactively after detecting unusual activity on the network. Upon detection, we immediately took all systems offline and took steps to investigate and determine the nature of the incident. Based on the results of that assessment, there is evidence to suggest an unauthorized third party accessed CMC's network. A comprehensive investigation was also conducted to identify any instances of sensitive data compromise so that we could contact individuals who may have been affected by this incident.

This letter serves to notify you that it is possible the following personal information could have been compromised by an unauthorized third party: first and last name, mailing address, Social Security number, date of birth, demographic information, and medical information maintained by CMC.

What We Are Doing:

Upon detecting this incident, we moved quickly to initiate a response, which included conducting an investigation with the assistance of cybersecurity experts, confirming the security of our network environment, and notifying law enforcement. CMC has also reviewed and altered our policies and procedures relating to the security of our systems and servers, and reviewed and altered how we manage data within our network.

We are offering free identity monitoring services through Kroll, a leading identity protection technology company. Kroll services include: 12 months of Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. With this protection, Kroll will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to activate the free Kroll services by going to <https://enroll.krollmonitoring.com>. If you need assistance with activation, please call our dedicated call center, managed by Kroll at 1-???-???-?????. Your membership number is <<Membership Number s_n>>. Please note the deadline to activate these services is **February 4, 2022**.

1 **CERTIFICATE OF SERVICE**

2 I, Amanda Salas, the undersigned, do declare as follows:

3 I am a resident of the County of San Diego; I am over the age of 18 years, and not a party
4 to, or have any interest in, this legal action; my business address is 750 B Street, Suite 1820, San
5 Diego, California 92101.

6 On June 9, 2022, I served the following document(s):

7 **CORRECTED CONSOLIDATED CLASS ACTION COMPLAINT**

8 in the manner(s) identified below on all interested parties as indicated on the attached service list:

9 **(X) VIA ELECTRONIC MAIL** – I electronically transmitted a copy of the
10 document(s) listed above to all parties in a pdf or word processing format at their
11 respective electronic mailbox addresses, pursuant to consent to such form of service.

12 **() VIA U.S. MAIL** – I enclosed a copy of the document identified above in an
13 envelope or envelopes and placed the envelope(s) for collection and mailing on the date
14 and at the place shown above, following our ordinary business practices. I am readily
15 familiar with this business’s practice of collecting and processing correspondence for
16 mailing. On the same day that correspondence is placed for collection and mailing, it is
17 deposited in the ordinary course of business with the U.S. Postal Service, in a sealed
18 envelope with postage prepaid.

19 I declare under penalty of perjury under the laws of the State of California that the
20 foregoing is true and correct. Executed on this 9th day of June, 2022, at San Diego, California.

21
22
23
24
25

AMANDA SALAS

SERVICE LIST

ROBERT AHDOOT (SBN 172098)
TINA WOLFSON (SBN 174806)
AHDOOT & WOLFSON, PC
2600 W. Olive Ave. Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585
rahdoot@ahdootwolfson.com
twolfson@ahdootwolfson.com

BEN BARNOW
ANTHONY L. PARKHILL
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: (312) 621-2000
Fax: (312) 641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiff Robert Donaire
No. STK-CV-UBC-2021-10605

M. ANDERSON BERRY
GREGORY HAROUTUNIAN
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Tel.: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com
GHaroutunian@justice4you.com

DAVID K. LIETZ
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue, NW, Suite 440
Washington, DC 20015-2052
Tel: (866) 252-0878
Fax: (202) 686-2877
dlietz@milberg.com

GARY M. KLINGER
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@milberg.com

GARY E. MASON
DANIELLE L. PERRY
MASON LLP
5101 Wisconsin Avenue NW, Suite 305
Washington D.C. 20016
Tel: (202) 429-2290
Fax: (202) 429-2294
gmason@masonllp.com
dperry@masonllp.com

*Attorneys for Plaintiffs Christopher Beck, Mohammad M Dawood, and Sylvia Lopez
No. STK-CV-UBT-2021-0010482*

TERENCE R. COATES
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 665-0204
Facsimile: (513) 665-0219
tcoates@msdlegal.com

*Attorneys for Plaintiff Darin Palermo
Case No. STK-CV-UBT-2021-0010626*

MICHAEL F. RAM
MARIE N. APPEL
MORGAN & MORGAN COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Tel.: (415) 358-6913
Fax: (415) 358-6293
mram@forthepeople.com
mappel@forthepeople.com

JOHN A. YANCHUNIS
RYAN D. MAXEY
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmaxey@forthepeople.com

*Attorneys for Plaintiff Aholiva Justiniano Miranda
No. STK-CV-UCC-2021-0011353*

SCOTT EDWARD COLE
LAURA GRACE VAN NOTE
CODY ALEXANDER BOLCE
COLE & VAN NOTE
555 12th Street, Ste. 1725
Oakland, CA 94607
Tel.: (510) 891-9800
Fax: (510) 891-7030
sec@colevannote.com
lvn@colevannote.com
cab@colevannote.com

*Attorneys for Plaintiff Daniel Hinds
No. STK-CV-UNPI-2021-0010404*

DAVID ROSS
WILSON, ELSER, MOSKOWITZ, EDELMAN & DICKER LLP
1500 K Street, NW, Suite 330
Washington, D.C. 20005
Tel: (202) 626-7687
Fax: (202) 628-3606
david.ross@wilsonelser.com

EDWARD GARSON
KENDRA TIETJEN
WILSON, ELSER, MOSKOWITZ, EDELMAN & DICKER LLP
655 Montgomery St., Ste. 900
San Francisco, CA 94111
Tel.: (415) 433-0990
Fax: (415) 434-1370
Edward.Garson@wilsonelser.com
Kendra.Tietjen@wilsonelser.com

Attorneys for Defendant Community Medical Centers, Inc.