

1 Gustavo Ponce, Esq.  
Nevada Bar No. 15084  
2 Mona Amini, Esq.  
Nevada Bar No. 15381  
3 **KAZEROUNI LAW GROUP, APC**  
6787 W. Tropicana Avenue, Suite 250  
4 Las Vegas, Nevada 89103  
Telephone: (800) 400-6808  
5 Facsimile: (800) 520-5523  
E-mail: mona@kazlg.com  
6 *Attorneys for Plaintiff*

7 **UNITED STATES DISTRICT COURT**  
8 **DISTRICT OF NEVADA**

9 HEATHER HILLBOM, individually and on  
10 behalf of all others similarly situated,

11 Plaintiff,

12 vs.

13 R1 RCM, INC.; and DIGNITY HEALTH d/b/a  
14 DIGNITY HEALTH - ST. ROSE DOMINICAN  
HOSPITAL, ROSE DE LIMA CAMPUS,

15 Defendants.  
16  
17  
18  
19  
20

Case No.:

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

21 //  
22 //  
23 //  
24 //  
25 //  
26 //  
27 //  
28 //



**INTRODUCTION**

1  
2 1. Plaintiff Heather Hillbom (“Plaintiff”), individually and on behalf of all others  
3 similarly situated (collectively, the “Class members”) brings this class action against Defendants R1  
4 RCM, Inc. (“R1”) and Dignity Health d/b/a St. Rose Dominican Hospital, Rose de Lima Campus  
5 (“Dignity”) (jointly as “Defendants”), for their failure to secure and safeguard Plaintiff’s and  
6 approximately 16,120 similarly situated Class members’ personally identifying information (“PII”) and  
7 personal health information (“PHI”), including but not limited to their names, Social Security  
8 numbers, dates of birth, addresses, contact information, medical record numbers, patient account  
9 numbers, medical information, and location of services.

10 2. R1 is a third-party vendor of technology-based revenue cycle management services  
11 for hospitals, health systems, physician groups, and other entities in the healthcare industry.

12 3. Sometime between January 30, 2023, and November 17, 2023, an unauthorized third  
13 party gained access to R1’s network system and obtained files containing information about  
14 Dignity’s current and former patients, including Plaintiff and the Class (the “Data Breach”).

15 4. Defendants owed a duty to Plaintiff and Class members to implement and maintain  
16 reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against  
17 unauthorized access, disclosure, and exfiltration by unauthorized third parties. Defendants breached  
18 that duty by, among other things, failing to implement and maintain reasonable security procedures  
19 and practices to protect Plaintiff and other similarly situated Dignity patients’ PII/PHI from  
20 unauthorized access and disclosure.

21 5. As a result of Defendants’ inadequate data security and breach of their duties  
22 and obligations, the Data Breach occurred, and Plaintiff’s and Class members’ PII/PHI was accessed,  
23 disclosed, viewed, and exfiltrated by unauthorized third parties that took possession of Plaintiff’s and the  
24 Class members’ PII/PHI. Further, Plaintiff and the Class (defined below) have been placed in  
25 an imminent and continuing risk of harm from fraud, identity theft, and related harm  
26 caused by the Data Breach and should remain vigilant for any signs of fraud or identity  
27 theft for the indefinite future.

28



1 from this District and Defendant does business and transact business in this judicial district.

2 **PARTIES**

3 13. Plaintiff is a citizen and resident of the State of Nevada and in this judicial district.

4 14. Sometime prior to the Data Breach, Plaintiff was a patient of and obtained healthcare  
5 or related services from Dignity, including at its St. Rose Dominican Hospital, Rose de Lima  
6 Campus located in Henderson, Nevada. As a condition of receiving services, Dignity required  
7 Plaintiff to provide them with her PII/PHI.

8 15. Based on representations made by Dignity, and Plaintiff's reliance on such  
9 representations, Plaintiff believed Dignity had implemented and maintained reasonable security and  
10 practices to protect her PII/PHI from unauthorized access. Relying on Dignity's representations and  
11 her belief that her PII/PHI would be reasonably safeguarded, Plaintiff provided her PII/PHI to  
12 Dignity in connection with receiving healthcare services. Plaintiff's PII/PHI was entrusted to  
13 Defendants with the reasonable expectation and mutual understanding that Defendants would  
14 comply with its obligations to keep such information confidential and secure from unauthorized  
15 access.

16 16. Plaintiff takes great care to protect her PII/PHI. If Plaintiff had known that Dignity  
17 would not adequately protect the PII/PHI in its possession, including by contracting with companies  
18 that do not adequately protect the PII/PHI in their possession, she would not have agreed to entrust  
19 Dignity with her PII/PHI or obtained healthcare services from Dignity.

20 17. Plaintiff received a letter from Defendants, dated March 11, 2024, informing  
21 Plaintiff, in relevant portion, of the following:

22 R1 RCM Inc. ("R1") is providing this notice to you on behalf of St. Rose  
23 Dominican Hospital de Lima, a Dignity Health hospital ("Dignity")  
24 regarding an incident that may have impacted the privacy of your  
25 protected health information ("PHI"). R1 is contacting you because we are  
26 a business associate of Dignity and processed your PHI in the course of  
27 providing those services. This notice provides information about the  
28 incident, the actions we are taking out of an abundance of caution and  
what to do if you have further questions."

R1 became aware on November 17, 2023 that PHI associated with Dignity  
was in the possession of an unauthorized third party (the "Dignity PHI").  
R1 immediately began an investigation into the matter and determined a  
copy of this PHI was present on a server maintained by CloudMed, an R1  
company, when the server was targeted by the exploitation of a zero-day

1 vulnerability of GoAnywhere software by the same unauthorized third  
2 party on January 30, 2023 (the “GoAnywhere Event”). While we could  
3 not definitively confirm that the GoAnywhere Event was the source of the  
4 PHI at issue, we are nonetheless providing this notice out of an abundance  
5 of caution.

6 R1 undertook an analysis of the Dignity PHI and on, January 11, 2024,  
7 determined that certain PHI, including your name, contact information,  
8 date of birth, Social Security number, location of services, clinical and/or  
9 diagnosis information and patient account and/or medical record number  
10 was potentially included in the Dignity PHI.

11 In connection with R1’s response to the GoAnywhere Event, R1 rebuilt  
12 the impacted server and implemented the patch released by GoAnywhere  
13 in February 2023 designed to address the vulnerability at issue. In  
14 addition, out of an abundance of caution, we have secured the services of  
15 Kroll to provide two years of identity monitoring services at no cost to  
16 you.

17 18. Since learning of the Data Breach, Plaintiff has undertaken reasonable efforts to  
18 mitigate the impact of the Data Breach, including but not limited to reviewing her accounts and  
19 credit reports for any indications of fraud or identity theft, freezing her credit, and replacing debit or  
20 cards. As a result of the Data Breach, Plaintiff will continue to spend valuable time for the  
21 remainder of her life, to mitigate the impact of the Data Breach, and dispute and rectify the fraud  
22 and/or damage to her credit reputation experienced as a result of the Data Breach which Plaintiff  
23 otherwise would have spent on other activities, including but not limited to leisure, work, and/or  
24 recreation.

25 19. Since the Data Breach, Plaintiff has noticed unauthorized credit inquiries on her  
26 credit report, and learned that her PII were found on the dark web, which Plaintiff believes to be  
27 attributed to the Data Breach. In addition, Plaintiff has spent time and incurred costs enrolling in  
28 credit monitoring and identity theft protection services in order to further mitigate the impact of the  
Data Breach.

20. As a direct result of the Data Breach, Plaintiff has suffered injury and damages  
including, *inter alia*, invasion of privacy, a substantial and imminent risk of identity theft and  
medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive  
PII/PHI; deprivation of the value of her PII/PHI; and overpayment for services that did not include  
adequate data security. Plaintiff and the Class has incurred and will continue to incur this damage in  
addition to any fraudulent use of their sensitive personal information, including their PII/PHI, for

1 years to come.

2 21. Defendant R1 is a Delaware corporation with a corporate headquarters or principal  
3 place of business at 433 W. Ascension Way Suite 200, Murray, Utah 84123.

4 22. Defendant Dignity Health is headquartered in San Francisco, California, and  
5 operates numerous hospitals, including St. Rose Dominican Hospital, Rose de Lima Campus  
6 located in Henderson, Nevada.

7 **FACTUAL ALLEGATIONS**

8 ***PII/PHI Is a Valuable Property Right that Must Be Protected***

9 23. In a Federal Trade Commission (“FTC”) roundtable presentation, former  
10 Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by  
11 observing:

12 Most consumers cannot begin to comprehend the types and amount of  
13 information collected by businesses, or why their information may be  
14 commercially valuable. Data is currency. The larger the data set, the  
greater potential for analysis – and profit.<sup>1</sup>

15 24. The value of PII as a commodity is measurable. “PII, which companies obtain at  
16 little cost, has quantifiable value that is rapidly reaching a level comparable to the value of  
17 traditional financial assets.”<sup>2</sup> It is so valuable to identity thieves that once PII has been disclosed,  
18 criminals often trade it on the “cyber black-market” for several years.

19 25. Companies recognize PII as an extremely valuable commodity akin to a form of  
20 personal property. For example, Symantec Corporation’s Norton brand has created a software  
21 application that values a person’s identity on the black market.<sup>3</sup>

22 26. As a result of its real value and the recent large-scale data breaches, identity thieves  
23 and cyber criminals openly post credit card numbers, Social Security numbers, PII and other  
24 sensitive information directly on various illicit Internet websites making the information publicly  
25

26 <sup>1</sup> FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC  
27 Exploring Privacy Roundtable) (Dec. 7, 2009), <https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable>.

28 <sup>2</sup> See Soma, *Corporate Privacy Trend, supra*.

<sup>3</sup> Risk Assessment Tool, Norton 2010, [www.everyclickmatters.com/victim/assessment-tool.html](http://www.everyclickmatters.com/victim/assessment-tool.html).

1 available for other criminals to take and use. This information from various breaches, including the  
 2 information exposed in the Data Breach, can be aggregated and become more valuable to thieves  
 3 and more damaging to victims. In one study, researchers found hundreds of websites displaying  
 4 stolen PII and other sensitive information. Strikingly, none of these websites were blocked by  
 5 Google’s safeguard filtering mechanism – the “Safe Browsing list.”

6 27. Recognizing the high value that consumers place on their PII, some companies now  
 7 offer consumers an opportunity to sell this information to advertisers and other third parties. The  
 8 idea is to give consumers more power and control over the type of information they share – and  
 9 who ultimately receives that information. By making the transaction transparent, consumers will  
 10 make a profit from the surrender of their PII.<sup>4</sup> This business has created a new market for the sale  
 11 and purchase of this valuable data.<sup>5</sup>

12 28. Consumers place a high value not only on their PII, but also on the privacy of that  
 13 data. Researchers shed light on how much consumers value their data privacy – and the amount is  
 14 considerable. Indeed, studies confirm that “when privacy information is made more salient and  
 15 accessible, some consumers are willing to pay a premium to purchase from privacy protective  
 16 websites.”<sup>6</sup>

17 29. One study on website privacy determined that U.S. consumers valued the restriction  
 18 of improper access to their PII between \$11.33 and \$16.58 per website.<sup>7</sup>

19 30. Given these facts, any company that transacts business with a consumer and then  
 20 compromises the privacy of consumers’ PII has thus deprived that consumer of the full monetary  
 21 value of the consumer’s transaction with the company.  
 22  
 23

24 <sup>4</sup> Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010)  
 available at <https://www.nytimes.com/2010/07/18/business/18unboxed.html>.

25 <sup>5</sup> See Julia Angwin and Emil Steel, *Web’s Hot New Commodity: Privacy*, Wall Street Journal  
 (Feb. 28, 2011) available at <https://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

26 <sup>6</sup> Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An  
 Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), available at  
 27 <https://www.jstor.org/stable/23015560?seq=1#>

28 <sup>7</sup> II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation*  
 (Mar. 2003) at table 3, available at <https://ideas.repec.org/p/wpa/wuwpio/0304001.html> (emphasis  
 added).



1 *Theft of PII/PHI Has Grave and Lasting Consequences for Victims*

2 31. A data breach is an incident in which sensitive, protected, or confidential data has  
3 potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers  
4 rely on the internet and apps on their phone and other devices to conduct every-day transactions,  
5 data breaches are becoming increasingly more harmful.

6 32. The United States Government Accountability Office noted in a June 2007 report on  
7 Data Breaches (“GAO Report”) that identity thieves use PII to take over existing financial accounts,  
8 open new financial accounts, receive government benefits and incur charges and credit in a person’s  
9 name.<sup>8</sup> As the GAO Report states, this type of identity theft is so harmful because it may take time  
10 for the victim to become aware of the theft and can adversely impact the victim’s credit rating.

11 33. In addition, the GAO Report states that victims of identity theft will face “substantial  
12 costs and inconveniences repairing damage to their credit records ... [and their] good name.”  
13 According to the FTC, identity theft victims must spend countless hours and large amounts of  
14 money repairing the impact to their good name and credit record.<sup>9</sup>

15 34. Identity thieves use personal information for a variety of crimes, including credit  
16 card fraud, phone or utilities fraud, and bank/finance fraud.<sup>10</sup> According to Experian, “[t]he research  
17 shows that personal information is valuable to identity thieves, and if they can get access to it, they  
18 will use it” to among other things: open a new credit card or loan; change a billing address so the  
19 victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and  
20 write bad checks; use a debit card number to withdraw funds; obtain a new driver’s license or ID;  
21 use the victim’s information in the event of arrest or court action.<sup>11</sup>

22 \_\_\_\_\_  
23 <sup>8</sup> See GAO, GAO Report 9 (2007) available at <http://www.gao.gov/new.items/d07737.pdf>.

24 <sup>9</sup> See FTC Identity Theft Website: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

25 <sup>10</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying  
26 information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes  
27 “identifying information” as “any name or number that may be used, alone or in conjunction with  
28 any other information, to identify a specific person,” including, among other things, “[n]ame, social  
security number, date of birth, official State or government issued driver's license or identification  
number, alien registration number, government passport number, employer, or taxpayer  
identification number.” *Id.*

<sup>11</sup> See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How  
Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), available at





1 35. Social Security numbers, for example, are among the worst kind of personal  
2 information to have stolen because they may be put to a variety of fraudulent uses and are difficult  
3 for an individual to change. The Social Security Administration stresses that the loss of an  
4 individual's Social Security number, as is the case here, can lead to identity theft and extensive  
5 financial fraud:

6 A dishonest person who has your Social Security number can use it to get  
7 other personal information about you. Identity thieves can use your  
8 number and your good credit to apply for more credit in your name. Then,  
9 they use the credit cards and don't pay the bills, it damages your credit.  
10 You may not find out that someone is using your number until you're  
turned down for credit, or you begin to get calls from unknown creditors  
demanding payment for items you never bought. Someone illegally using  
your Social Security number and assuming your identity can cause a lot of  
problems.<sup>12</sup>

11 36. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report,  
12 the average cost of a data breach per consumer was \$150 per record.<sup>13</sup> Other estimates have placed  
13 the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity  
14 theft – a common result of data breaches – was \$298 dollars.<sup>14</sup> And in 2019, Javelin Strategy &  
15 Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket  
16 cost to consumers for identity theft was \$375.<sup>15</sup>

17 37. A person whose PII has been compromised may not see any signs of identity theft  
18 for years. According to the GAO Report:

19 "[L]aw enforcement officials told us that in some cases, stolen data may  
20 be held for up to a year or more before being used to commit identity theft.  
21 Further, once stolen data have been sold or posted on the Web, fraudulent  
22 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."

23  
24 <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

25 <sup>12</sup> Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

26 <sup>13</sup> Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

27 <sup>14</sup> Norton By Symantec, 2013 Norton Report 8 (2013), *available at* [https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton\\_raportti.pdf](https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf).

28 <sup>15</sup> Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (citing the Javelin report).



1 38. For example, in 2012, hackers gained access to LinkedIn’s users’ passwords.  
2 However, it was not until May 2016, four years after the breach, that hackers released the stolen  
3 email and password combinations.<sup>16</sup>

4 39. PHI is particularly valuable and has been referred to as a “treasure trove for  
5 criminals.”<sup>17</sup> A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten  
6 personal identifying characteristics of an individual.”<sup>18</sup>

7 40. All-inclusive health insurance dossiers containing sensitive health insurance  
8 information, names, addresses, telephone numbers, email addresses, SSNs, and bank account  
9 information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each on  
10 the black market.<sup>19</sup>

11 41. According to a report released by the Federal Bureau of Investigation’s (“FBI”) Cyber  
12 Division, criminals can sell healthcare records for 50 times the price of a stolen Social  
13 Security or credit card number.<sup>20</sup>

14 42. It is within this context that Plaintiff and thousands of similar individuals must now  
15 live with the knowledge that their PII/PHI is forever in cyberspace, putting them at imminent and  
16 continuing risk of damages, and was taken by unauthorized persons willing to use the information  
17 for any number of improper purposes and scams, including making the information available for  
18 sale on the dark web and/or the black market.

19 ***Defendants and their Collection of PII/PHI***

20 43. Upon information and belief, R1 is “a business associate of Dignity and processed  
21 [Plaintiff’s] PHI in the course of providing those services” to Dignity.<sup>21</sup>

22 \_\_\_\_\_  
23 <sup>16</sup>See Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), available at  
24 <https://blog.linkedin.com/2016/05/18/protecting-our-members>.

25 <sup>17</sup> See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20,  
26 2019) <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>  
27 <sup>18</sup> *Id.*

28 <sup>19</sup> See SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC  
MAG. (July 16, 2013), [https://www.scmagazine.com/news/breach/health-insurance-credentials-  
fetch-high-prices-in-the-online-black-market](https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market).

<sup>20</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for  
Increased Cyber Intrusions for Financial Gain* (April 8, 2014), [https://www.illumweb.com/wp-  
content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf](https://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf).

<sup>21</sup> <https://www.mass.gov/doc/assigned-data-breach-number-2024-477-r1-rcm-inc/download>

1 44. Upon information and belief, Dignity used R1 for revenue cycle management  
2 services.<sup>22</sup>

3 45. Plaintiff and Class members are current or former patients of Dignity and entrusted  
4 Dignity with their PII/PHI, including but not limited to the PII/PHI compromised by the Data  
5 Breach.

6 *The Data Breach*

7 46. Between approximately January 30, 2023, and November 17, 2023, “an unauthorized  
8 third party” gained access to “protected health information (“PHI”) associated with Dignity.”<sup>23</sup>

9 47. According to the Notice of Cybersecurity Incident posted on Dignity’s website,<sup>24</sup> the  
10 PII/PHI affected in the Data Breach compromised the patient name, contact information, date of  
11 birth, location of services, clinical and/or diagnosis information, patient account and/or medical  
12 record number, and Social Security number, of Plaintiff and the Class members.

13 48. Defendants reported to the U.S. Department of Health and Human Services’ Office  
14 for Civil Rights that on “3/11/2024,” R1 reported an “Hacking/IT Incident” involving a “Network  
15 Server” affecting “16121” individuals.

16 49. Dignity’s Notice of Privacy Practices states, “We understand that your protected  
17 health information is private and personal. We are committed to protecting it...We are required by  
18 law to keep your protected health information private...[and] notify you as outlined in state and  
19 federal law if a breach of your unsecured protected health information has occurred.”<sup>25</sup>

20 50. R1 became aware of the data breach on November 17, 2023; and, based on  
21 Defendants’ data breach notice letter, the Data Breach occurred as early as January 30, 2023. Thus,  
22 it is possible that it took over nine (9) months for Defendants to even realize the Data Breach  
23 occurred. However, Defendants failed to notify Plaintiff and the Class members until on or around  
24 March 11, 2024, almost four (4) months after their knowledge of the Data Breach.

25 \_\_\_\_\_  
26 <sup>22</sup> <https://www.dignityhealth.org/las-vegas/website-notice/r1-provides-notice-of-cybersecurity-incident>

27 <sup>23</sup> *Id.*

28 <sup>24</sup> *Id.*

<sup>25</sup> <https://www.dignityhealth.org/content/dam/dignity-health/pdfs/hipaa-notice-of-privacy-practices/Notice%20of%20Privacy%20Practices%20DH%20NV%2010.2020.pdf>

1 51. Defendants’ failure to both promptly discover and notify Plaintiff and Class  
2 members that their PII/PHI was accessed and stolen by unauthorized third parties allowed those  
3 who were able to obtain their PII/PHI to monetize, misuse, or disseminate that PII/PHI before  
4 Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a  
5 result, Plaintiff and the Class members have and will continue to suffer indefinitely from the  
6 damage of substantial, imminent, and concrete risk that their identities will be, or already have been,  
7 stolen and misused by unauthorized third parties.

8 52. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA  
9 covered entities to provide notification following a breach of unsecured protected health  
10 information. Following a breach of unsecured protected health information, covered entities must  
11 provide notification of the breach to affected individuals. Covered entities must *only* provide the  
12 required notifications if the breach involved unsecured protected health information. Unsecured  
13 protected health information is protected health information that has not been rendered unusable,  
14 unreadable, or indecipherable to unauthorized persons through the use of a technology or  
15 methodology specified by the Secretary of the U.S. Dept. of Health and Human Services in  
16 guidance. Under approved guidance of the U.S. Dept. of Health and Human Services, protected  
17 health information (“PHI”) is rendered unusable, unreadable, or indecipherable to unauthorized  
18 individuals if (1) electronic PHI has been encrypted as specified in the HIPAA Security Rule by  
19 “the use of an algorithmic process to transform data into a form in which there is a low probability  
20 of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of  
21 encryption) and (2) such confidential process or key that might enable decryption has not been  
22 breached. By reporting this incident to the U.S. Dept. of Health and Human Services, by sending its  
23 data breach notification letter, Defendants have determined and affirmed that Plaintiff’s and the  
24 Class Members’ electronic PII/PHI was either not encrypted at all, or if it was encrypted, the  
25 encryption has been breached by the unauthorized third party. As a result, Defendants were  
26 negligent for failing to encrypt or adequately encrypt Plaintiff’s and the Class Members’ electronic  
27 medical information.  
28



1 53. Plaintiff's and Class Members' unencrypted PII/PHI may end up for sale on the dark  
2 web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted  
3 marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily  
4 access the PII and PHI of Plaintiff and Class Members.

5 54. Defendants did not use reasonable security procedures and practices appropriate to  
6 the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class  
7 Members, causing their PII and PHI to be exposed, accessed, disclosed, viewed, and taken by  
8 unauthorized parties.

9 55. As a condition of its relationships with Plaintiff and Class Members, Defendants  
10 required that Plaintiff and Class Members entrust Defendants with highly confidential PII and PHI.

11 56. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members,  
12 Defendants assumed legal and equitable duties and knew or should have known that it was  
13 responsible for protecting the PII and PHI from unauthorized access, disclosure, viewing, and  
14 exfiltration.

15 57. Plaintiff and Class Members took reasonable steps to maintain the confidentiality of  
16 their PII and PHI and relied on Defendants to keep their PII and PHI confidential and securely  
17 maintained, to use this information for business purposes only, and to make only authorized  
18 disclosures of such sensitive and private personal information.

19 58. Defendants could have prevented this Data Breach by properly safeguarding and  
20 encrypting the PII and PHI of Plaintiff and Class Members. In addition, to the extent permissible,  
21 Defendants could have destroyed the data, especially old data from former patients.

22 59. Despite the prevalence of public announcements of data breach and data security  
23 compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiff and  
24 Class Members from being compromised in the Data Breach.

25 60. As a result of the Data Breach and Defendants' conduct and/or omissions, Plaintiff  
26 and Class members have suffered and will suffer injury, including, but not limited to: (i) a  
27 substantially increased and imminent risk of identity theft; (ii) the unauthorized disclosure and theft  
28 of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery



1 from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting  
2 to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their  
3 PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and  
4 money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as  
5 a result of the Data Breach; and (vii) overpayment for services that were received without adequate  
6 data security to reasonably safeguard Plaintiff and the Class members' PII/PHI from unauthorized  
7 disclosure, access, and exfiltration.

8 **CLASS ACTION ALLEGATIONS**

9 61. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks to represent and  
10 intends to seek certification of a class (the "Class") defined as:

11 **All individuals whose PII/PHI was impacted by the Data Breach,**  
12 **including all individuals who were sent a notice of the Data Breach by**  
13 **or on behalf of Defendants.**

14 62. Excluded from the Class are: (1) Defendants and their respective officers, directors,  
15 employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the  
16 agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such  
17 persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of  
18 their immediate families.

19 63. Certification of Plaintiff's claims for class wide treatment is appropriate because  
20 Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as  
21 would be used to prove those elements in individual actions alleging the same claims.

22 64. Plaintiff reserves the right to, after conducting discovery, modify, expand, or amend  
23 the above Class definition or to seek certification of a class or Classes defined differently than  
24 above before any court determines whether certification is appropriate.

25 65. The Class members are so numerous and geographically dispersed throughout  
26 California that joinder of all Class members would be impracticable. While the exact number of  
27 Class members is unknown, based on information and belief, the Class consists of tens of thousands  
28 of individuals, including Plaintiff and the Class members. Plaintiff therefore believe that the Class is

1 so numerous that joinder of all members is impractical.

2 66. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed  
3 members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members  
4 were injured by the same wrongful acts, practices, and omissions committed by Defendants, as  
5 described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that  
6 give rise to the claims of all Class members.

7 67. There is a well-defined community of interest in the common questions of law and  
8 fact affecting Class members. The questions of law and fact common to Class members  
9 predominate over questions affecting only individual Class members, and include without  
10 limitation:

- 11 a) Whether Defendants had a duty to implement and maintain reasonable security  
12 procedures and practices appropriate to the nature of the PII/PHI it collected, stored,  
13 and maintained from Plaintiff and Class members;
- 14 b) Whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class  
15 members to unauthorized third parties;
- 16 c) Whether Defendants failed to exercise reasonable care to secure and safeguard  
17 Plaintiff's and Class members' PII/PHI;
- 18 d) Whether Defendants breached their duty to protect the PII/PHI of Plaintiff and each  
19 Class member; and
- 20 e) Whether Plaintiff and each Class member are entitled to damages and other equitable  
21 relief.

22 68. Plaintiff will fairly and adequately protect the interests of the Class members.  
23 Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to or that  
24 conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial  
25 experience and success in the prosecution of complex consumer protection and consumer privacy  
26 class actions of this nature.

27 69. A class action is superior to any other available method for the fair and efficient  
28 adjudication of this controversy since individual joinder of all Class members is impractical.



1 Furthermore, the expenses and burden of individual litigation would make it difficult or impossible  
2 for the individual members of the Class to redress the wrongs done to them, especially given that  
3 the damages or injuries suffered by each individual member of the Class are outweighed by the  
4 costs of suit. Even if the Class members could afford individualized litigation, the cost to the court  
5 system would be substantial and individual actions would also present the potential for inconsistent  
6 or contradictory judgments. By contrast, a class action presents fewer management difficulties and  
7 provides the benefits of single adjudication and comprehensive supervision by a single court.

8 70. Defendants have acted or refused to act on grounds generally applicable to the entire  
9 Class, thereby making it appropriate for this Court to grant final injunctive, including public  
10 injunctive relief, and declaratory relief with respect to the Class as a whole.

11 **CAUSES OF ACTION**

12 **COUNT I**

13 **NEGLIGENCE**

14 71. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully  
15 set forth herein.

16 72. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care  
17 in safeguarding and protecting the PII/PHI in their possession, custody, or control.

18 73. In addition, Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule  
19 ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and  
20 Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection  
21 of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C  
22 (collectively, "HIPAA Privacy and Security Rules"). Defendants' duties also arise from Section 5 of  
23 the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting  
24 commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as  
25 Defendants, of failing to employ reasonable measures to protect and secure Plaintiff and the Class  
26 members' PII/PHI.

27 74. Defendants' violation of the HIPAA Privacy and Security Rules and Section 5 of  
28 the FTCA constitutes negligence *per se*.

1 75. Defendants knew or should have known the risks of collecting and storing Plaintiff’s  
2 and all other Class members’ PII/PHI and the importance of maintaining secure systems.  
3 Defendants knew or should have known of the many data breaches that targeted healthcare providers  
4 that collect and store PII/PHI in recent years.

5 76. Given the nature of Defendants’ businesses, the sensitivity and value of the PII/PHI  
6 they maintain, and the resources at their disposal, Defendants should have identified the  
7 vulnerabilities to their systems or their third-party vendor’s systems and prevented the Data Breach  
8 from occurring.

9 77. Defendants breached these duties by failing to, or contracting with companies that  
10 failed to, exercise reasonable care in safeguarding and protecting Plaintiff’s and Class members’  
11 PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement,  
12 control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls,  
13 policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI  
14 entrusted to it—including Plaintiff’s and Class members’ PII/PHI.

15 78. It was reasonably foreseeable for Defendants that their failure to exercise reasonable  
16 care in safeguarding and protecting Plaintiff’s and Class members’ PII/PHI by failing to, or  
17 contracting with companies that failed to, design, adopt, implement, control, direct, oversee,  
18 manage, monitor, and audit appropriate data security processes, controls, policies, procedures,  
19 protocols, and software and hardware systems would result in the unauthorized release, disclosure,  
20 and dissemination of Plaintiff’s and Class members’ PII/PHI to unauthorized individuals.

21 79. As a result of Defendants’ above-described wrongful actions, inaction, and want of  
22 ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members  
23 have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the  
24 likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-  
25 pocket expenses associated with the prevention, detection, and recovery from unauthorized  
26 use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the  
27 actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which  
28 remains in Defendants’ possession; (vi) future costs in terms of time, effort, and money that will be



1 required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data  
2 Breach; and (vii) overpayment for the services that were received without adequate data security  
3 measures implemented by Defendants.

4 **COUNT II**

5 **BREACH OF IMPLIED CONTRACT**

6 80. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully  
7 set forth herein.

8 81. In connection with receiving healthcare services, Plaintiff and all other Class  
9 members entered into implied contracts with Dignity, who contracted with R1.

10 82. Plaintiff and Class members paid money to Dignity, directly or through their  
11 insurance, and provided Dignity with their PII/PHI pursuant to said implied contracts. In exchange,  
12 Dignity agreed, and Plaintiff and Class members understood, that among other things, Dignity  
13 would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect  
14 the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) safeguard  
15 Plaintiff's and Class members' PII/PHI in compliance with state and federal laws, regulations, and  
16 industry standards.

17 83. The protection of PII/PHI was a material term of the implied contracts between  
18 Plaintiff and Class members, on the one hand, and Dignity, on the other hand. Indeed, as set forth  
19 supra, Dignity recognized the importance of data security and the privacy of Dignity's patients'  
20 PII/PHI.

21 84. Had Plaintiff and Class members known that Dignity would not adequately protect  
22 their PII/PHI, they would not have agreed to provide their PII/PHI to Dignity or received healthcare  
23 or other services from Dignity, which they were required to pay for, and Dignity received  
24 compensation for in return.

25 85. Plaintiff and Class members performed their obligations under the implied contract  
26 when they provided Dignity with their PII/PHI and paid for healthcare or other services from  
27 Dignity.

28 86. Dignity breached its implied contracts with Plaintiff and the Class members in



1 failing to implement and maintain reasonable security measures to protect and safeguard their  
2 PII/PHI, including by ensuring companies it contracts with implement and maintain reasonable  
3 security measures to protect PII/PHI, and in failing to implement and maintain security protocols  
4 and procedures to protect Plaintiff's and Class members' PII/PHI in a manner complying with  
5 applicable state and federal laws, regulations, and industry standards.

6 87. Dignity's breach of its obligations of its implied contracts with Plaintiff and Class  
7 members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class  
8 members have suffered from the Data Breach.

9 88. Plaintiff and all other Class members were damaged by Dignity's breach of implied  
10 contracts because: (i) they paid—directly or through their insurers—for data security protection  
11 they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—  
12 risks justifying expenditures for protective and remedial services for which they are entitled to  
13 compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the  
14 confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their  
15 PII/PHI, for which there is a well-established national and international market; (vi) lost time and  
16 money incurred to mitigate and remediate the effects of the Data Breach, including the increased  
17 risks of identity theft they face and will continue to face; and (vii) overpayment for services that  
18 were received without adequate data security.

19 **COUNT III**

20 **UNJUST ENRICHMENT**

21 89. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully  
22 set forth herein.

23 90. Defendants received a monetary benefit from Plaintiff and the Class members in the  
24 form of monies paid to Dignity for healthcare services, which Dignity used in turn to pay for R1's  
25 services, and which was centered around Plaintiff and the Class members providing their PII/PHI in  
26 order to receive such healthcare services.

27 91. Defendants accepted and/or had knowledge of the benefits conferred upon them by  
28 Plaintiff and Class members; and Defendants both benefitted from the receipt of Plaintiff's and

1 Class members' PII/PHI, as it was used during R1's services provided to Dignity.

2 92. As a result of Defendants' conduct, Plaintiff and Class members suffered actual  
3 damages in an amount equal to the difference in value between their payments made with  
4 reasonable data privacy and security practices and procedures that Plaintiff and Class members paid  
5 for without reasonable data privacy and security practices and procedures that they received.

6 93. Plaintiff and the Class members would remain injured, and Defendants would be  
7 unjustly enriched if they were permitted to retain money belonging to Plaintiff and the Class  
8 members because Defendants failed to adequately implement the data privacy and security  
9 procedures that Plaintiff and Class members paid for and that were otherwise required pursuant to  
10 state and federal laws, regulations, and industry standards.

11 94. Defendants should be disgorged of all unlawful proceeds received by them from  
12 Plaintiff and the Class members in light of their unlawful conduct and Data Breach caused by their  
13 inadequate data security.

14 95. Plaintiff and the Class members are entitled to equitable relief as they have no  
15 adequate remedy at law for their injuries suffered, and continuing to accrue, as a result of  
16 Defendants' unlawful conduct and Data Breach caused by their inadequate data security.

17 **PRAYER FOR RELIEF**

18 96. Plaintiff, individually and on behalf of the Class, respectfully requests that (i) this  
19 action be certified as a class action, (ii) Plaintiff be designated a representative of the Class,  
20 (iii) Plaintiff's counsel be appointed as counsel for the Class.

21 97. Plaintiff, individually and on behalf of the Class, further requests that upon final trial  
22 or hearing, judgment be awarded against Defendants as follows:

- 23
- 24 • actual and punitive damages to be determined by the trier of fact;
  - 25 • equitable relief, including restitution, as may be appropriate;
  - 26 • injunctive relief, including remedial measures to be implemented by Defendants  
27 designed to prevent such a data breach by adopting improved data security  
28 practices necessary to safeguard Plaintiff and the Class members' PII/PHI and

1 extended identity theft protection and credit monitoring services design o protect  
2 Plaintiff and the Class members from identity theft and fraud;

- 3 • declaratory relief, as may be appropriate;
- 4 • pre- and post-judgment interest at the applicable legal rates;
- 5 • attorneys' fees, litigation expenses, and costs of suit; and
- 6 • any such other and further relief the Court deems just and proper.

7 **DEMAND FOR JURY TRIAL**

8 98. Plaintiff hereby demands a jury trial on all issues so triable.

9  
10 DATED this 5th day of April 2024.

11 Respectfully submitted,

12 **KAZEROUNI LAW GROUP, APC**

13  
14 By: /s/ Mona Amini  
15 Mona Amini, Esq.  
16 Gustavo Ponce, Esq.  
17 6787 W. Tropicana Ave., Suite 250  
18 Las Vegas, Nevada 89103

19 *Attorneys for Plaintiff*



# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Lawsuit Alleges R1 RCM, Dignity Health Failed to Protect Patient Data from Cyberattack](#)

---