

ELECTRONICALLY FILED  
Polk County Circuit Court  
Michelle Schnell, Circuit Clerk  
2023-Jan-13 14:44:56  
57CV-23-12  
AS C18WD01 : 28 Pages

**IN THE CIRCUIT COURT OF POLK COUNTY, ARKANSAS**  
**DIVISION**

CHRIS CANT and TIMOTHY CRAIG, on behalf of themselves and all others similarly situated,

Plaintiff,

v.

MENA REGIONAL HEALTH SYSTEM, d/b/a MENA HOSPITAL COMMISSION and JOHN DOE INSURANCE CARRIER,

Defendants.

Case No. 57CV-23-12

**COMPLAINT - CLASS ACTION**

Jury Trial Demanded

Plaintiffs Chris Cant and Timothy Craig (“Plaintiffs”) bring this Class Action Complaint on behalf of themselves, and all others similarly situated, against Defendants Mena Regional Health System d/b/a Mena Regional Hospital Commission (“Mena Regional”) and John Doe Insurance Carrier (collectively with Mena Regional, “Defendants”), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

**NATURE OF THE ACTION**

1. Healthcare providers that handle sensitive, personally identifying information (“PII”) or protected health information (“PHI”) owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person’s PII or PHI through a

data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. Mena Regional is a healthcare system that operates both in- and out-patient facilities in Polk County, Arkansas, Western Arkansas, and Eastern Oklahoma.<sup>1</sup> Mena Regional employs more than 76 people and generates approximately \$14 million in annual revenue.<sup>2</sup>

4. As a healthcare provider, Mena Regional knowingly obtains sensitive patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

5. Mena Regional's Privacy Notice for Health Information Practices states that it "[e]ach time [a patient] visit[s] a hospital, physician, or other health care provider, a record of [the patient's] visit is made" and Mena Regional "will not use or disclose [patient] health information without [ ] authorization."<sup>3</sup> Mena Regional's Privacy Notice does not authorize it to disclose patient information to unauthorized third-parties.

---

<sup>1</sup> *Who We Are*, Mena Regional Health System, <https://menaregional.com/about-us/who-we-are/> (last visited Dec. 14, 2022).

<sup>2</sup> *Mena Regional Health System Reports Leaked SSNs and PHI Following Data Breach*, JDSUPRA (Dec. 1, 2022), <https://www.jdsupra.com/legalnews/mena-regional-health-system-reports-3199091/>.

<sup>3</sup> *Mena Regional Health System Privacy Notice for Health Information Practices*, Mena Regional Health System (last updated May 2014), <https://www.menaregional.com/wp-content/uploads/2016/07/MRHSNPPMAY2014.pdf>.

6. On November 22, 2022, Mena Regional notified its patients that their PII and PHI stored on its systems had accessed and exfiltrated by an unauthorized third-party (the “Data Breach”).<sup>4</sup>

7. Despite an unauthorized third-party accessing and removing patient PII and PHI on or about October 31, 2021, Mena Regional did not identify the Data Breach until November 8, 2022, more than a year after the Data Breach occurred.<sup>5</sup>

8. Based on the public statements of Mena Regional to date, a wide variety of PII and PHI was implicated in the Data Breach, including but not limited to patient names, dates of birth, Social Security numbers, driver’s license/government identification numbers, financial account information, medical record/patient account number(s), medical diagnosis/treatment information, medical provider name(s), lab results, prescription information, and health insurance information.<sup>6</sup>

9. As a direct and proximate result of Mena Regional’s failure to implement and follow basic security procedures, Plaintiffs’ and Class Members’ PII and PHI is now in the hands of cybercriminals.

10. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

---

<sup>4</sup> *Notice of Data Security Incident*, Mena Regional Health System (Nov. 22, 2022), <https://menaregional.com/notice-of-data-security-incident/>.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

11. Plaintiffs, on behalf of themselves, and all others similarly situated, alleges claims for negligence, negligence *per se*, and declaratory judgment. Plaintiffs seek damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard PII and PHI in Mena Regional's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

### PARTIES

12. Plaintiff Chris Cant is an adult who, at all relevant times, is a resident and a citizen of the State of Arkansas. Plaintiff was a patient of Mena Regional. Plaintiff received a Data Breach Notification informing him that his PII and PHI he provided to Mena Regional had been compromised in the Data Breach.

13. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of her PII and PHI—time which he would not have had to expend but for the Data Breach.

14. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

15. Plaintiff Timothy Craig is an adult who, at all relevant times, is a resident and a citizen of the State of Arkansas. Plaintiff was a patient of Mena Regional. Plaintiff received a Data Breach Notification informing him that his PII and PHI he provided to Mena Regional had been compromised in the Data Breach.

16. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of her PII and PHI—time which he would not have had to expend but for the Data Breach.

17. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

18. Defendant Mena Regional is a citizen-owned healthcare organization believed to be under the direction of the Mena Hospital Commission, a governmental commission formed by the City of Mena, Arkansas.

19. Should Mena Regional be entitled to immunity, Plaintiffs hereby bring a direct action against John Doe Insurance Company, a liability carrier for Mena Regional, pursuant to Arkansas Code Annotated § 23-79-210. Said John Doe Insurance Company is named pursuant to Arkansas Code Annotated § 16-56-125, because at the time of filing this Complaint, Plaintiffs are unaware of the exact identity of all possible insurance policies providing coverage for the acts and omissions alleged herein.

20. In the event that Mena Regional seeks and is determined to be entitled to immunity, Plaintiffs assert a direct action against John Doe Insurance Company as set forth in the preceding paragraph of this Complaint.

### **JURISDICTION AND VENUE**

21. This Court has jurisdiction over Defendant because it does business in Arkansas, including but not limited to operating a hospital in the state.

22. Venue in this county is proper as the Defendant is located in this county, the dispute that gave rise to this lawsuit occurred in this county.

### **FACTUAL BACKGROUND**

#### **A. Mena Regional and the Services It Provides.**

23. Mena Regional “offer[s] a diverse compliment of inpatient and outpatient services to the communities of Polk County, Western Arkansas and Eastern Oklahoma.”<sup>7</sup> Mena Regional’s “[i]npatient services include[:] acute care medical/surgical services, a six bed ICU, labor and delivery, a 12 bed geriatric psychiatry unit (Mena Senior Behavioral Health Center) and a 12 bed acute care physical rehabilitation unit (Mena Rehabilitation Center)” and its “[o]utpatient services include[:] Ouachita Rehabilitation Center, dermatology, cardiology, ophthalmology and urology clinics.”<sup>8</sup>

24. While providing these healthcare services, Mena Regional receives, creates, and handles PII and PHI, which includes, *inter alia*, patient names, dates of birth, Social Security numbers, driver’s license/government identification numbers, financial account information, medical record/patient account number(s), medical diagnosis/treatment information, medical provider name(s), lab results, prescription information, and health insurance information.

25. Patients must entrust their PII and PHI to Mena Regional in order to receive healthcare services, and in return, they reasonably expect that Mena Regional will safeguard their highly sensitive information and keep their PHI confidential.

26. Even though Mena Regional “is committed to maintaining the privacy of personal information in its possession” and the “privacy and security of the personal information [Mena Regional] maintains is of the utmost importance”<sup>9</sup> it nevertheless employed inadequate data security measures to protect and secure the PII and PHI patients entrusted to it, resulting in the Data Breach and compromise of Plaintiffs’ and Class Members’ PII and PHI.

---

<sup>7</sup> *Who We Are*, Mena Regional Health System, <https://menaregional.com/about-us/who-we-are/> (last visited Dec. 14, 2022).

<sup>8</sup> *Id.*

<sup>9</sup> *Notice of Data Security Incident*, *supra* note 4.

**B. Mena Regional Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims.**

27. Mena Regional was well aware that the PHI and PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

28. Mena Regional also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

29. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

30. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been “proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce.”<sup>10</sup> PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

31. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.<sup>11</sup>

---

<sup>10</sup> Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), <http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/>.

<sup>11</sup> *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), <https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/>.

32. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.<sup>12</sup>

33. The healthcare industry has become a prime target for threat actors: “High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks.”<sup>13</sup>

34. Additionally, “[h]ospitals store an incredible amount of patient data. Confidential data that’s worth a lot of money to hackers who can sell it on easily – making the industry a growing target.”<sup>14</sup>

35. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenu found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenu compiled in 2020.<sup>15</sup>

36. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security’s mid-year report released in July. The percentage of

---

<sup>12</sup> *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20> (last visited Dec. 14, 2022).

<sup>13</sup> *The healthcare industry is at risk*, SwivelSecure <https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/> (last visited Dec. 14, 2022).

<sup>14</sup> *Id.*

<sup>15</sup> *2022 Breach Barometer*, PROTENUS, <https://www.protenus.com/breach-barometer-report> (last visited Dec. 14, 2022).



healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.<sup>16</sup>

37. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Mena Regional's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

38. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from \$20 say up to—we've even seen \$60 or \$70."<sup>17</sup> A complete identity theft kit that includes health insurance credentials may be worth up to \$1,000 on the black market, whereas stolen payment card information sells for about \$1.<sup>18</sup>

39. According to Experian:

Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

ID theft victims often have to spend money to fix problems related to having their data stolen, which averages \$600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly \$13,500

---

<sup>16</sup> Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: <https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year>.

<sup>17</sup> *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, New Ponemon Study Shows, IDX (May 14, 2015), <https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat>.

<sup>18</sup> *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security<sup>®</sup> Survey 2015*, PriceWaterhouseCoopers, <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf> (last visited Dec. 14, 2022).

dealing with their hassles, which can include the cost of paying off fraudulent medical bills.

Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.<sup>19</sup>

40. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: “[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] 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.”<sup>20</sup>

41. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

---

<sup>19</sup> Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/>.

<sup>20</sup> U.S. Gov't Accountability Office, *Report to Congressional Requesters, Personal Information, June 2007*: <https://www.gao.gov/new.items/d07737.pdf> (last visited Dec. 14, 2022).

42. Based on the value of its patients' PII and PHI to cybercriminals, Mena Regional certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

**C. Mena Regional Breached its Duty to Protect its Patient PII and PHI.**

43. On or about October 31, 2021, Mena Regional announced that it was "investigating a recent security incident that impacted a limited portion [its] network."<sup>21</sup>

44. After conducting an investigation into the incident with the assistance of a third-party expert, Mena Regional discovered nearly a year later, on November 8, 2022, that it was subjected to the Data Breach, which occurred on or about October 30, 2021.<sup>22</sup>

45. During the Data Breach, an unauthorized third-party gained access to and exfiltrated Mena Regional files containing patient PII and PHI.<sup>23</sup>

46. The nature of the information compromised in the Data Breach includes full names, dates of birth, Social Security numbers, driver's license/government identification numbers, financial account information, medical record/patient account number(s), medical diagnosis/treatment information, medical provider name(s), lab results, prescription information, and health insurance information.<sup>24</sup>

47. On November 22, 2022, over a year after the Data Breach, Mena Regional reported the Data Breach to the Department of Health and Human Services Office for Civil Rights ("HHS").<sup>25</sup>

---

<sup>21</sup> Ethan Nahte, *MRHS victim of security incident*, My Pulse News (Dec. 1, 2021), <https://mypulsenews.com/mrhs-victim-of-security-incident/>.

<sup>22</sup> *Notice of Data Breach*, *supra* note 4.

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

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

<sup>25</sup> *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Dep't of Health & Human Services, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (last visited Dec. 14, 2022).

48. All in all, nearly 85,000 patients of Mena Regional had their PII and/or PHI breached.<sup>26</sup>

49. The Data Breach occurred as a direct result of Mena Regional's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect its patients' PII and PHI.

50. On or about the same date that Mena Regional reported the Data Breach to HHS, Mena Regional provided notice to Plaintiffs indicating that their PII and PHI may have been accessed and/or exfiltrated during the Data Breach.

51. Like Plaintiffs, the Class Members received similar notices informing them that their PII and/or PHI was exposed and/or exfiltrated in the Data Breach.

**D. Mena Regional is Obligated Under HIPAA to Safeguard Personal Information.**

52. Mena Regional is required by the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1302d, *et seq.* ("HIPAA") to safeguard patient PHI.

53. Mena Regional is an entity covered by under HIPAA, which sets minimum federal standards for privacy and security of PHI.

54. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

55. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

---

<sup>26</sup> *Id.*

56. Under C.F.R. 160.103, HIPAA defines “individually identifiable health information” as “a subset of health information, including demographic information collected from an individual” that is (1) “created or received by a health care provider;” (2) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;” and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

57. HIPAA requires Mena Regional to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA’s security requirements. 45 CFR § 164.102, *et. seq.*

58. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Mena Regional to provide notice of the Data Breach to each affected individual “without unreasonable delay and in no case later than 60 days following discovery of the breach.”<sup>27</sup>

59. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiffs or the Class Members consent to the disclosure of their PHI to cybercriminals.

---

<sup>27</sup> *Breach Notification Rule*, U.S. Dep’t of Health & Human Services, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>.

60. As such, Mena Regional is required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that it acquires, receives, and collects, and Mena Regional is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

61. Given the application of HIPAA to Mena Regional, and that Plaintiffs and Class Members entrusted their PHI to Mena Regional in order to receive healthcare services, Plaintiffs and Class Members reasonably expected that Mena Regional would safeguard their highly sensitive information and keep their PHI confidential.

**E. FTC Guidelines Prohibit Mena Regional from Engaging in Unfair or Deceptive Acts or Practices.**

62. Mena Regional is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

63. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.<sup>28</sup>

64. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no

---

<sup>28</sup> *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.<sup>29</sup>

65. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.<sup>30</sup>

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. Mena Regional was at all times fully aware of its obligations to protect the PII and PHI of patients because of its position as a healthcare provider, which gave it direct access to reams of patient PII and PHI. Mena Regional was also aware of the significant repercussions that would result from its failure to do so.

68. Despite its obligations, Mena Regional failed to properly implement basic data security practices and Mena Regional's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

---

<sup>29</sup> *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personalinformationpdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformationpdf).

<sup>30</sup> *Id.*

**F. Plaintiffs and Class Members Suffered Damages.**

69. For the reasons mentioned above, Mena Regional's conduct, which allowed the Data Breach to occur, caused Plaintiffs and members of the Class significant injuries and harm in several ways. Plaintiffs and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

70. Once PII and PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Mena Regional's conduct. Further, the value of Plaintiffs and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

71. As a result of Mena Regional's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

72. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.<sup>31</sup>

---

<sup>31</sup> Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, <https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud> (last visited Dec. 14, 2022).



73. With respect to healthcare breaches, another study found “the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft.”<sup>32</sup>

74. “Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data’s utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures.”<sup>33</sup>

75. The reality is that cybercriminals seek nefarious outcomes from a data breach and “stolen health data can be used to carry out a variety of crimes.”<sup>34</sup>

76. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.<sup>35</sup>

77. “Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous.”<sup>36</sup>

---

<sup>32</sup> Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, HealthITSecurity, <https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breachesincreases-risk-of-fraud> (last visited Dec. 14, 2022).

<sup>33</sup> *Id.*

<sup>34</sup> Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>.

<sup>35</sup> *Id.*

<sup>36</sup> *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, Experian, <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf> (last visited Dec. 14, 2022).

78. Plaintiffs and Class Members are also at a continued risk because their information remains in Mena Regional's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Mena Regional fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

79. Plaintiffs and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

### **CLASS ALLEGATIONS**

80. Plaintiffs bring this class action on behalf of herself and all other individuals who are similarly situated pursuant to Rule 23 of the Arkansas Rules of Civil Procedure.

81. Plaintiffs seek to represent a class of persons to be defined as follows:

All individuals whose PII and/or PHI was compromised in the Mena Regional Data Breach which was announced on or about November 22, 2022 (the "Class").

82. Excluded from the Class are Defendants, their subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

83. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

84. **Numerosity:** Plaintiffs are informed and believes, and thereon alleges, that there are at minimum, hundreds of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Mena Regional's records,

including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately hundreds of individuals.

85. **Commonality:** This action involves questions of law and fact common to the Class. Such common questions include but are not limited to:

- a. Whether Defendants had a duty to protect the PII and PHI of Plaintiffs and Class Members;
- b. Whether Defendants were negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI, and breached their duties thereby;
- c. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and
- d. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

86. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class were all patients of Mena Regional, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

87. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

88. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

89. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendants breached their duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

90. **Injunctive Relief** – Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Rule 23 of Arkansas Civil Procedure.

91. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Mena Regional's books and records.

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

92. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

93. Defendants owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

94. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

95. Defendants have a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendants. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

96. Defendants' duty also arose from Defendants' position as a healthcare provider. Defendants hold themselves out as a trusted provider of healthcare, and thereby assume a duty to reasonably protect their patients' information. Indeed, Defendants who provide healthcare services were in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

97. Defendants breached the duties owed to Plaintiffs and Class Members and thus were negligent. As a result of a successful attack directed towards Defendants that compromised Plaintiffs' and Class Members' PII and PHI, Defendants breached their duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external

risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices published to their patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

98. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised.

99. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered injuries, including:

- a. Theft of their PII and/or PHI;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual

- and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;
- f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;
  - g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;
  - h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and
  - i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

100. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

**SECOND CAUSE OF ACTION**  
**NEGLIGENCE PER SE**  
**(On Behalf of Plaintiffs and the Class)**

101. Plaintiffs restate and reallege all preceding factual allegations above as if fully set forth herein.

102. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair acts or practices by entities such as Defendants for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants’ duty.

103. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendants’ conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of their patients.

104. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

105. Defendants’ violation of Section 5 of the FTC Act constitutes negligence *per se*.

106. Defendants are an entity covered under HIPAA which sets minimum federal standards for privacy and security of PHI.

107. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendants have a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff’s and the Class Members’ electronic PHI.

108. Specifically, HIPAA required Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the



PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq.*

109. Defendants violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

110. Plaintiffs and the Class Members are patients within the class of persons HIPAA was intended to protect.

111. Defendants' violation of HIPAA constitutes negligence *per se*.

112. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

113. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured as described herein and in Paragraph 97 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

**THIRD CAUSE OF ACTION**  
**DECLARATORY JUDGMENT**  
**(On Behalf of Plaintiffs and the Class)**

114. Plaintiffs restate and reallege all preceding allegations above as if fully set forth herein.

115. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

116. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendants are currently maintaining

data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII will occur in the future.

117. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendants owe a legal duty to secure patients' PII and PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and HIPAA; and
- b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

118. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

119. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

120. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by

employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

121. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiffs and consumers whose confidential information would be further compromised.

### **PRAYER FOR RELIEF**

WHEREFORE Plaintiffs on behalf of themselves and all other similarly situated, prays for relief as follows:

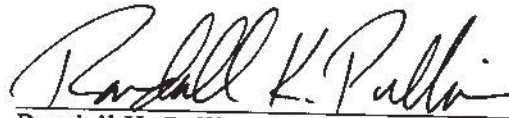
- a. For an order certifying the Class under Rule 23 of the State Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;
- c. For damages in an amount to be determined by the trier of fact;
- d. For an order of restitution and all other forms of equitable monetary relief;
- e. Declaratory and injunctive relief as described herein;
- f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;
- g. Awarding pre- and post-judgment interest on any amounts awarded; and,
- h. Awarding such other and further relief as may be just and proper.

### **JURY TRIAL DEMAND**

A jury trial is demanded on all claims so triable.

Dated: January 12, 2023

Respectfully submitted,



Randall K. Pulliam (AR Bar 981105)  
Courtney E. Ross (AR Bar 2021156)  
**CARNEY BATES & PULLIAM, PLLC**  
519 West 7<sup>th</sup> Street  
Little Rock, AR 72201  
Telephone: 501-312-8500  
Facsimile: 501-312-8505  
[rpulliam@cbplaw.com](mailto:rpulliam@cbplaw.com)  
[cross@cbplaw.com](mailto:cross@cbplaw.com)

Gary F. Lynch (*pro hac vice forthcoming*)  
**LYNCH CARPENTER, LLP**  
1133 Penn Avenue, 5th Floor  
Pittsburgh, PA 15222  
Telephone: (412) 322-9243  
Facsimile: (412) 231-0246  
[gary@lcllp.com](mailto:gary@lcllp.com)

*Counsel for Plaintiffs and the Class*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Mena Regional Facing Class Action Over Data Breach Affecting Nearly 85K Patients](#)

---