DraUNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

IRIS KALE individually and on behalf of all others similarly situated, Plaintiff, v. MEDICAL ASSOCIATES OF THE LEHIGH VALLEY, P.C., Defendant.	**CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Iris Kale ("Plaintiff") individually and on behalf of all others similarly situated, brings this action against Medical Associates of the Lehigh Valley ("MATLV" or "Defendant"), a Pennsylvania professional corporation, to obtain damages, restitution, and injunctive relief for herself and for the Class, as defined below, from Defendant.

Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") and protected health information ("PHI") of its patients and employees, including, without limitation: names, addresses, email addresses, birth dates, Social Security numbers, driver's license numbers, state ID numbers, health insurance provider names, medical diagnoses, treatment information, medications, and lab results.[1]

2. Defendant is Pennsylvania's largest primary care group dedicated to preserving the

[1] HIPAA Journal, *Ransomware Attack on Medical Associates of the Lehigh Valley Affects 75K Patients*, available at https://www.hipaajournal.com/ransomware-attack-on-medical-associates-of-the-lehigh-valley-affects-75k-patients/, Sept. 14, 2022 (last accessed Nov. 9, 2022).

private practice model as a physician owned professional corporation.[2]

3. In order to obtain medical treatment, Plaintiff and other patients and employees of Defendant entrust and provide to Defendant an extensive amount of PII. Defendant also records an extensive amount of PHI regarding its patients, including diagnoses and treatment information. Defendant retains this information on its network systems—even long after the treatment relationship ends. Defendant acknowledges that it understands the importance of protecting information.

4. MATLV detected a ransomware attack on its network on or around July 3, 2022 (the "Data Breach").[3]

5. On September 9, 2022, two months later, Defendant filed notice of the Data Breach with the U.S. Department of Health and Human Services Office for Civil Rights and sent out data breach letters to the 75,628 patients affected by the breach.[4]

6. The unauthorized actors accessed and exfiltrated the PII and PHI of current and former MATLV patients ("Class Members"), including that of Plaintiff and Class Members.

7. It wasn't until September 9, 2022, two months after the Data Breach, until Defendant announced that the Data Breach had occurred.[5]

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. Defendant

---

[2] Medical Associates of the Lehigh Valley, *About Us*, available at https://www.matlv.com/content_view.asp?wid=1 (last accessed Nov. 9, 2022).

[3] JD Supra, *Medical Associates of the Lehigh Valley Reports Data Breach Affecting the SSNs and PHI of 75,628 Individuals*, available at https://www.jdsupra.com/legalnews/medical-associates-of-the-lehigh-valley-4405240/, Sept. 14, 2022 (last accessed Nov. 9, 2022).

[4] *Id.*

[5] *Id.*

admits that the PII and PHI accessed and exfiltrated included names, addresses, email addresses, birth dates, Social Security numbers, driver's license numbers, state ID numbers, health insurance provider names, medical diagnoses, treatment information, medications, and lab results.

9. The purpose of the Data Breach was the same as it is for many other data events: the exposed PII and PHI of Defendant's current and former patients can now be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Defendant's current and former patients face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

10. This PII and PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Defendant's current and former patients and employees.

11. Until notified of the breach, Plaintiff and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

12. Plaintiff brings this action on behalf of all persons whose PII and/or PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Defendant's current and former patients; (ii) warn Defendant's current and former patients of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered numerous actual and imminent injuries

as a direct result of the Data Breach, including: (a) theft of their PII and PHI; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' PII and PHI against theft and not allow access and misuse of their personal data by others; and (h) the continued risk to their PII and PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII and PHI, and, at the very least, are entitled to nominal damages.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Defendant's current and former patients' and employees' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was compromised through access by cybercriminals. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

I. PARTIES

15. Plaintiff Iris Kale is a citizen of Pennsylvania residing in Lehigh County, Pennsylvania. Plaintiff Kale has received Defendant's letter notifying her of the Data Breach.

16. Defendant Medical Associates of the Lehigh Valley, P.C. is a professional corporation organized under the laws of Pennsylvania, headquartered at 1605 N. Cedar Crest Blvd., Ste. 110, Allentown, PA 18104, with its principal place of business in Allentown, PA.

17. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

II. JURISDICTION AND VENUE

1. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's Pennsylvania citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs

2. The Court has personal jurisdiction over Defendant because Defendant's primary place of business is located within this District.

3. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant is incorporated in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2).

III. FACTUAL ALLEGATIONS

Background

4. Defendant operates over forty healthcare facilities throughout central Pennsylvania and offers a wide variety of health services, including pediatrics, physical therapy, disease management, osteopathic manipulation, diagnostics, sleep medicine, and more.

5. Defendant was founded in 1993 as an independent physician-owned professional corporation and has grown over the last three decades to include independent physicians and group practices in over 25 locations across the Commonwealth.[6]

6. Plaintiff and Class Members treated by Defendant were required to entrust some of their most sensitive and confidential information, including names, addresses, email addresses, birth dates, Social Security numbers, driver's license numbers, state ID numbers, health insurance provider names, medical diagnoses, treatment information, medications, and lab results. This includes information that is static, does not change, and can be used to commit myriad financial crimes.

7. In providing treatment to Plaintiff and Class Members, Defendant generated and retained additional sensitive personal information about Plaintiff and Class Members, including information concerning medical conditions, treatments, and diagnoses.

8. Plaintiff and Class Members, as current and former patients of Defendant, relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Defendant's current and former patients and employees demand security to safeguard their PII and PHI.

9. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from involuntary disclosure to third parties.

The Data Breach

[6] Medical Associates of the Lehigh Valley, *About Us,* available at https://www.matlv.com/content_view.asp?wid=1 (last accessed Nov. 9, 2022).

10. Defendant maintains both a "HIPAA Policy and Consent Form" (the "HIPAA Policy")[7] and an "Updated HIPAA Notice of Privacy Practices" (the "Privacy Notice") [8] on its website (collectively, the "Privacy Policies").

11. The HIPAA Policy promises that, "Your information will be kept confidential except as is necessary to provide services or to ensure that all administrative matters related to your care are handled appropriately."[9]

12. The Privacy Notice also provides a list of instances that disclosure of medical information could be made without prior written authorization – none of which are applicable here.[10]

13. Defendant's Privacy Notice further states that, "Other uses and disclosures not described in this [Privacy Notice] will be made only with authorization."[11]

14. Prior to the Data Breach, Defendant should have (i) encrypted or tokenized the sensitive PII and PHI of Plaintiff and Class Members, (ii) deleted such PII and PHI that it no longer had reason to maintain, (iii) eliminated the potential accessibility of the PII and PHI from the

---

[7] Medical Associates of the Lehigh Valley, *HIPAA Policy and Consent Form,* available at https://www.matlv.com/secure/cms/wysiwyg/assets/Docs/HIPAA%20Policy%20and%20Consent%20Information%202017.pdf (last accessed Nov. 9, 2022).

[8] Medical Associates of the Lehigh Valley, *Updated HIPAA Notice of Privacy Practices,* available at https://www.matlv.com/secure/cms/wysiwyg/assets/Docs/HIPAA%20Notice%20of%20Privacy%20Practices%20March%202013.pdf (last accessed Nov. 9, 2022).

[9] Medical Associates of the Lehigh Valley, *HIPAA Policy and Consent Form,* available at https://www.matlv.com/secure/cms/wysiwyg/assets/Docs/HIPAA%20Policy%20and%20Consent%20Information%202017.pdf (last accessed Nov. 9, 2022).

[10] Medical Associates of the Lehigh Valley, *Updated HIPAA Notice of Privacy Practices,* available at https://www.matlv.com/secure/cms/wysiwyg/assets/Docs/HIPAA%20Notice%20of%20Privacy%20Practices%20March%202013.pdf (last accessed Nov. 9, 2022).

[11] *Id*.

internet where such accessibility was not justified, and (iv) otherwise reviewed and improved the security of its network system that contained such PII and PHI.

15. Prior to the Data Breach, Defendant did not (i) encrypt or tokenize the sensitive PII and PHI of Plaintiff and the Class Members, (ii) delete such PII and PHI that it no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII and PHI from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of its network system that contained such PII and PHI.

16. At some point on or before July 3, 2022, an intruder gained unauthorized access to Defendant's network and attempted to shut down its computer network. Investigation revealed that some of the files accessed contained personal information of patients and who those patients may be.[12]

17. On or around September 9, 2022, Defendant publicly acknowledged the Data Breach.[13]

18. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former patients, causing the access and/or exfiltration of the PII and PHI of Plaintiff and the Class Members.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII and PHI.

19. Defendant acquired, collected, and stored Defendant's current and former patients' PII and PHI.

---

[12] JD Supra, *Medical Associates of the Lehigh Valley Reports Data Breach Affecting the SSNs and PHI of 75,628 Individuals*, available at https://www.jdsupra.com/legalnews/medical-associates-of-the-lehigh-valley-4405240/, Sept. 14, 2022 (last accessed Nov. 9, 2022).

[13] *Id.*

20. As a condition of maintaining treatment with Defendant, Defendant requires that its patients and/or employees entrust Defendant with highly confidential PII and PHI.

21. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

22. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI. Plaintiff and the Class Members, as current and former patients, relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

23. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiff's and Class Members' PII and PHI, or Defendant could have destroyed the data, especially old data from former patients that Defendant had no legal right or responsibility to retain.

24. Defendant's negligence in safeguarding Defendant's current and former patients' PII and PHI is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially in the healthcare sector.

25. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and the proposed Class from being compromised.

26. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with 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."[15]

27. The ramifications of Defendant's failure to keep secure Defendant's current and former patients' and employees' PII and PHI are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information and Protected Health Information

28. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[16] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[17] Criminals can also purchase access

[14] 17 C.F.R. § 248.201 (2013).

[15] *Id*.

[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 29, 2021).

[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, available at https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, Dec. 6, 2017 (last accessed June 26, 2022).

to entire company data breaches from $900 to $4,500.[18]

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

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

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

31. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited

[18] *In the Dark*, VPNOverview, available at https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 26, 2022).

[19] Social Security Administration, *Identity Theft and Your Social Security Number*, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 26, 2022).

into the new Social Security number."[20]

32. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, address, date of birth, driver's license number, medical information and history, and Social Security number.

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

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

35. The PII and PHI of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

36. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S.

[20] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed June 26, 2022).

[21] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, available at https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html, Feb. 6, 2015 (last accessed June 26, 2022).

Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in 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 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.[22]

37. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Defendant's current and former patients' and employees' PII and PHI, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Defendant's current and former patients and employees as a result of a breach.

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

39. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, potentially amounting to millions of individuals' detailed and confidential personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

40. Defendant has offered no aid to affected individuals like Plaintiff and the Class Members.

41. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and

[22] *Report to Congressional Requesters*, GAO, at 29, available at http://www.gao.gov/new.items/d07737.pdf, June 2007 (last accessed June 29, 2022).

PHI of Defendant's current and former patients and employees.

Plaintiff's Experience

42. Plaintiff is a former patient of Defendant. As a condition of treatment, she was required to provide and entrust her PII and PHI, including but not limited to her name, date of birth, address, phone number, email address, financial or bank account information, Social Security number, and insurance information and account number.

43. At the time of the Data Breach, Defendant retained the names, Social Security numbers, and PHI of Plaintiff and other individuals in its internal, administrative system.

44. Since the Data Breach, Plaintiff has received increased spam and phishing attempts. Plaintiff has received messages attempting to lure her into providing additional financial information via phone, text, and email; these attempts at defrauding the Plaintiff have only occurred after the Data Breach.

45. As a result of these fraud attempts, Plaintiff has spent time dealing with the consequences of the Data Beach, which includes time spent verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

46. Additionally, Plaintiff is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

47. Plaintiff stores any documents containing her PII and PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

48. Plaintiff has suffered actual injury in the form of lost time in addressing these fraud attempts in addition to the actual and imminent injury arising from damages to and diminution in

the value of her PII and PHI—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of her treatment, which was compromised in and as a result of the Data Breach.

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

50. Plaintiff has suffered and will continue to suffer injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third-parties and criminals.

51. Plaintiff has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

IV. CLASS ALLEGATIONS

52. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated pursuant to Rules 1701-1706 of the Pennsylvania Rules of Civil Procedure on behalf of herself and all others similarly situated.

53. The Class that Plaintiff seeks to represent is defined as follows:

> **All individuals whose PII and/or PHI was accessed and/or exfiltrated during the Data Breach (the "Class").**

54. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

55. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

56. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

57. Numerosity: The Class is so numerous that joinder of all members is impracticable. On information and believe, the class size approximately 75,628 individuals; in any event, the exact numbers of members in the Class can be ascertained through Defendant's records.

58. Commonality: Questions of law and fact common to the Classe exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

59. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of herself and the other Class Members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

60. Typicality: Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendant's misfeasance. Defendant's misconduct impacted all Class Members in the same manner and arose from the same set of operative facts and are based on the same set of legal theories.

61. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that

would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

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

63. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause

of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

66. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members and Defendant may continue to act unlawfully as set forth in this Complaint.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

67. Plaintiff realleges and incorporates by reference all of the allegations contained herein.

68. As a condition of their treatment or employment by Defendant, Defendant's current and former patients and employees were obligated to provide and entrust Defendant with certain PII and PHI, including their names, Social Security numbers, driver's license numbers, state ID numbers, addresses, email addresses, medical insurance information, and health and treatment information.

69. Plaintiff and the Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

70. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Class could and would suffer if the PII and/or PHI were wrongfully disclosed.

71. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former patients' and employees PII and PHI involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

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

73. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' and employees' PII and PHI it was no longer required to retain pursuant to regulations.

74. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII and PHI.

75. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII and PHI, a necessary part of obtaining treatment or employment from Defendant.

76. Defendant were subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class.

77. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

78. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendant's systems.

79. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques freely available to Defendant.

80. Plaintiff and the Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

81. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

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

83. Defendant had a duty to employ proper procedures to prevent the unauthorized

dissemination of the PII and PHI of Plaintiff and the Class.

84. Defendant has admitted that the PII and PHI of Plaintiff and the Class was wrongfully accessed by and exfiltrated by unauthorized third persons as a result of the Data Breach.

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

86. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

87. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former patients' and employees' PII and PHI in the face of increased risk of theft.

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

89. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former patients' and employees' PII and PHI it was no longer required to retain pursuant to regulations.

90. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

91. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and

the Class, the PII and PHI of Plaintiff and the Class would not have been compromised.

92. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiff and the Class and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Class's PII and PHI was accessed and exfiltrated as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

93. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

94. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

95. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

96. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

97. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

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

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

100. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to further

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

101. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class Members are at an increased risk of identity theft or fraud.

102. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is entitled to and demand actual consequential, and nominal damages and injunctive relief.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

103. Plaintiff realleges and incorporates by reference all of the allegations contained herein.

104. Defendant offered medical and healthcare services to Plaintiff and Class Members in exchange for compensation and other benefits.

105. Defendant acquired and maintained the PII and PHI of Plaintiff and the Class, including names, addresses, email addresses, birth dates, Social Security numbers, driver's license numbers, state ID numbers, health insurance provider names, medical diagnoses, treatment information, medications, and lab results.

106. At the time Defendant acquired the PII and PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and PHI and not take unjustified risks when storing the PII and PHI.

107. Plaintiff and the Class would not have entrusted their PII and PHI to Defendant had they known that Defendant would make the PII and PHI internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII and PHI that Defendant no longer had a reasonable need to maintain.

108. Defendant was therefore required to reasonably safeguard and protect the PII and PHI of Plaintiff and the Class Members from unauthorized disclosure or use.

109. Plaintiff and the Class fully performed their obligations under their implied contracts with Defendant.

110. Plaintiff and the Class Members would not have provided and entrusted their PII and PHI to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII and PHI for uses other than services from Defendant.

111. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to protect and keep private medical information of Plaintiff and the Class, including failing to (i) encrypt or tokenize the sensitive PII and PHI of Plaintiff and the Class, (ii) delete such PII and PHI that it no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII and PHI from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII and PHI.

112. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

113. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff is at an increased risk of identity theft or fraud.

114. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff is entitled to and demands actual, consequential, and nominal damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

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

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

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to

the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

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

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with

additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient

to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

Date: November 11, 2022

Respectfully Submitted,

/s/ *James A. Barry*
James A. Barry
PA Attorney ID: 209524
Joshua M. Neuman
PA Attorney ID: 322648
POGUST GOODHEAD, LLC
505 S. Lenola Rd., Suite 126
Moorestown, New Jersey 08057
(610) 941-4204
jbarry@pogustgoodhead.com
jneuman@pogustgoodhead.com

Todd S. Garber (pro hac vice forthcoming)
Andrew White (pro hac vice forthcoming)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Seth A. Meyer (pro hac vice forthcoming)
Alex J. Dravillas (pro hac vice forthcoming)
KELLER POSTMAN LLC
150 N. Riverside, Suite 4100
Chicago, Illinois 60606
Tel.: (312) 741-5220
sam@kellerpostman.com
ajd@kellerpostman.com

ClassAction.org