UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

TANYA DARDEN, *individually and on behalf of all others similarly situated*, Plaintiff, v. **UNIVERSITY HOSPITALS HEALTH SYSTEM, INC., *doing business as* UNIVERSITY HOSPITALS,** Defendant.	No. 1: 26-cv-02830 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, Tanya Darden ("Plaintiff"), on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendant, University Hospitals Health System, Inc., d/b/a University Hospitals, ("University Hospitals" or "Defendant"):

NATURE OF THE ACTION

1. This Class Action arises from a cyberattack that was discovered by Defendant on October 22, 2026, resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach"). On information and belief, the Breach affects over a million current and former patients.

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former patients' highly personal information, including their personally identifying information ("PII") as well as protected health information ("PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

3. Defendant has still not yet begun notifying Class Members about the Data Breach as of the time of filing of this Complaint. Instead, Defendant chose to issue statements to various

different news platforms acknowledging that it had been subject to a Data Breach ("Online Breach Statement").

4. Defendant continues delaying notice to Class Members even though Plaintiff and countless of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

5. Defendant Online Breach Statement intentionally obfuscated the nature of the breach and the threat it posted—how the breach happened, who it specifically impacted, and why Defendant continues to delay notifying victims that hackers had gained access to highly private Sensitive Information.

6. Defendant's failure to timely detect and continued delay in reporting the Data Breach made its patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

8. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed thousands of its current and former patients.

9. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class

trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiff is a current patient and Data Breach victim.

11. Accordingly, Plaintiff, on behalf of herself and a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

12. Plaintiff, Tanya Darden, is a natural person and citizen of Cleveland, Ohio, where she intends to remain.

13. Defendant is a nonprofit corporation incorporated under the law of Ohio with its principal place of business located at 11100 Euclid Avenue, Cleveland, Ohio 44106.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one class member and Defendant are of different states. And there are over 100 putative Class members.

15. This Court has personal jurisdiction over Defendant because it is headquartered in Ohio, regularly conducts business in Ohio, and has sufficient minimum contacts in Ohio.

16. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

University Hospitals

17. Defendant boasts that it is "home to some of the most prestigious clinical and research programs in the nation, with more than 3,000 active clinical trials and research studies underway. UH Cleveland Medical Center is perennially among the highest performers in national ranking surveys" and has "more than 50 health centers and outpatient facilities, and over 200 physician offices[.]"[1]

18. In collecting and maintaining its current and former patients' Sensitive Information, Defendant agreed it would safeguard the data in accordance with state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information.

19. Indeed, Defendant promises in its *HIPAA Notice of Privacy Practices* that it "is committed to protecting your medical information" and "protect[s] patient safety, welfare and confidentiality."[2]

20. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

---

[1] University Hospitals, *Community Health Needs Assessment 2025: Cuyahoga County* 6, https://www.uhhospitals.org/-/media/files/about-uh/community-benefit/chna-cuyahoga-2025.pdf (last visited Oct. 28, 2026).

[2] University Hospitals, *HIPAA Notice of Privacy Practices*, https://www.uhhospitals.org/patients-and-visitors/hipaa-notice-of-privacy-practices (last visited Oct. 28, 2026).

The Data Breach

21. Plaintiff is a current patient and is a data breach victim. As a condition of treatment as a patient there, Plaintiff provided Defendant with her Sensitive Information, including her name, health insurance information, medication information, treatment information, Social Security number, date of birth, and home address. This was used to facilitate treatment of Plaintiff. Defendant required Plaintiff to provide that Sensitive Information to obtain treatment and care.

22. On information and belief, Defendant collects and maintains patients' Sensitive Information in its computer systems. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

23. Defendant admits on its website that, "We are currently experiencing issues with MyChart, we apologize for any inconvenience, and we are working to restore access to MyChart as quickly as possible. If you need to contact your provider's office regarding questions on results, appointments or other information please reach out to your provider's office directly."[3]

24. According to its statements to various news platforms, Defendant admits it first detected unusual activity on its servers, on October 22, 2026, and was forced to disconnect from the internet as a precaution.[4]

25. Defendant admitted in a statement shared on October 26, 2026, four days since it first detected the Data Breach, "Patients still cannot access MyChart," and that there were

[3] University Hospitals, Home Page, https://www.uhhospitals.org/ [https://perma.cc/7AKW-K3EC].

[4] Naomi Diaz, *University Hospitals reschedules procedures as cyber incident disruptions continue*, Becker's Health IT (Oct. 26, 2026), https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/university-hospitals-reschedules-procedures-as-cyber-incident-disruptions-continue/ (last visited Oct. 28, 2026).

"challenges connecting to the UH network at some locations. We are encountering problems with insurance pre-authorizations, among other issues."[5]

26. In other words, Defendant's cyber and data security systems were so completely inadequate that it allowed cybercriminals to obtain files containing a treasure trove of hundreds of thousands of its patients' highly private Sensitive Information.

27. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

28. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not in fact follow industry standard practices in securing patients' Sensitive Information, as evidenced by the Data Breach.

29. Defendant places the onus of responsibility on Plaintiff and the Class, providing no assurances that it plans on implementing any additional security or changes to prevent a similar breach form occurring again in the future.

30. Defendant has still not yet begun notifying Class Members about the Data Breach as of the filing of this Complaint. Instead, Defendant chose to issue statements to various different news platforms acknowledging that it had been subject to a Data Breach.

31. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

[5] *Id*.

32. On information and belief, Defendant offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

33. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its patients' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

34. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[6]

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

35. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

36. In light of recent high profile data breaches at other healthcare and healthcare adjacent companies, Defendant knew or should have known that its electronic records and patients' Sensitive Information would be targeted by cybercriminals.

[6] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, Harvard Bus. Rev. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back (last visited Oct. 28, 2026).

37. In 2024, a record 3,158 data breaches occurred—exposing approximately 1,350,835,988 sensitive records (i.e., 211% increase year over year).[7]

38. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

39. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations have experienced cyberattacks.[9]

40. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Plaintiff's Experience

41. Plaintiff is a current patient and a data breach victim. As a condition of treatment as a patient there, Plaintiff provided Defendant with her Sensitive Information, including her name, health insurance information, medication information, treatment information, Social Security number, date of birth, and home address. This was used to facilitate treatment of Plaintiff. Defendant required Plaintiff to provide that Sensitive Information to obtain treatment and care.

---

[7] Identity Theft Resource Center, *2024 Data Breach Report*, at 6 (Feb. 4, 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport_Final_020325.pdf (last visited Oct. 28, 2026).

[8] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Oct. 28, 2026).

[9] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, Security (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Oct. 28, 2026).

42. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her.

43. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

44. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

45. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

46. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

47. Plaintiff have suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

48. Plaintiff suffered actual injury from the exposure of her Sensitive Information—which violates her rights to privacy.

49. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

50. Indeed, Defendant's Data Breach prevented Plaintiff from properly managing her health care as she was unable to access her MyChart account for a significant period of time, preventing Plaintiff from being able to seek adequate treatment and care with Defendant, communicate with her providers, set or view appointments, access her prior patient data.

51. Further and following the Data Breach, Plaintiff began receiving spam calls on the same phone number that Defendant possessed and that was likely stolen in this Data Breach. These spam calls identify Plaintiff by first and last name and claimed to require Plaintiff to confirm and "verify" various Sensitive Information, including Plaintiff's date of birth, Social Security Number, as well as her address. The Sensitive Information involved in these phishing and spam calls are the same information Defendant possessed and that was likely stolen by cybercriminals in this Data Breach.

52. Finally, shortly after the Breach, Defendant received an alert via Experian and TransUnion that an unknown individual was requesting access to her credit report. Specifically, on October 26, 2026, Plaintiff was notified that "We recently received a recent request to access credit score that has appeared to not be directly sent or authorized by you." This alert is further proof that her Sensitive Information is now in the hands of cybercriminals because of this Breach

53. Once an individual's Sensitive Information has been stolen by cybercriminals and is for sale and access on the dark web, as Plaintiff's Sensitive Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[10] On information and belief, the spam calls that Plaintiff is experiencing is a result of

[10] Ryan Toohil, *What do Hackers Do With Stolen Information?*, Aura (Sept. 5, 2023), https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited Oct. 28, 2026).

the Data Breach. Indeed, the information exposed by Defendant's data breach was more than enough for cybercriminals to use and gather additional information to send her spam calls.

54. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

55. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

56. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

57. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

58. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

59. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

60. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

61. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

62. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily

create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

63. Defendant disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

64. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

65. In 2024, the technology and communications conglomerate Cisco published its annual *Consumer Privacy Survey*[11] and *Data Privacy Benchmark Study*.[12] Therein, Cisco reported the following:

---

[11] Cisco, *Privacy Awareness: Consumers Taking Charge to Protect Personal: Cisco 2024 Consumer Privacy Survey*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited Oct. 28, 2026).

[12] Cisco, *Privacy as an Enabler of Customer Trust: Cisco 2024 Data Privacy Benchmark Study*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf (last visited Oct. 28, 2026).

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[13]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[14]

c. 89% of consumers stated that "I care about data privacy."[15]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[16]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[17]

66. Defendant knew or should have known that adequate implementation of cybersecurity and protection of Sensitive Information, including Plaintiff and the Class's Sensitive Information, was important to its patients.

Defendant failed to adhere to FTC guidelines.

67. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous

[13] *Cisco 2024 Consumer Privacy Survey*, at 3, *supra* note 11.

[14] *Cisco 2024 Data Privacy Benchmark Study*, at 3, *supra* note 12.

[15] *Cisco 2024 Consumer Privacy Survey*, at 9, *supra* note 11.

[16] *Id*.

[17] *Id*.

guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

68. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

69. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

70. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive 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.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

73. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [18]

74. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[19]

75. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

[18] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[19] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

76. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant Fails to Comply with Industry Standards

77. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

78. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

79. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

80. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

81. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its patients. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

82. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose Sensitive Information was compromised in the Data Breach, including all those who receive notice of the breach.

83. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

84. Plaintiff reserves the right to amend the class definition.

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

a. **Numerosity**. Plaintiff is representative of the Class, consisting of several thousand members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

   i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

   ii. 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;

   iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;

   iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

   v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

   vi. Whether the Data Breach caused Plaintiff's and the Class's injuries;

   vii. What the proper damages measure is; and

viii. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

86. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

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

87. Plaintiff realleges all previous paragraphs as if fully set forth below.

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

89. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Sensitive Information in a data breach. And here, that foreseeable danger came to pass.

90. Defendant has full knowledge of the sensitivity of the Sensitive Information and the types of harm that Plaintiff and the Class could and would suffer if their Sensitive Information was wrongfully disclosed.

91. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices.

After all, Defendant actively sought and obtained Plaintiff and Class Members' Sensitive Information.

92. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the Sensitive Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their Sensitive Information.

93. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

94. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Sensitive Information it was no longer required to retain under applicable regulations.

95. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Sensitive Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

96. Defendant's duty to use reasonable security measures arose because 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 Sensitive Information, a necessary part of obtaining services from Defendant.

97. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant hold vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Sensitive Information —whether by malware or otherwise.

98. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

99. Defendant improperly and inadequately safeguarded the Sensitive Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

100. Defendant breached these duties as evidenced by the Data Breach.

101. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' Sensitive Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

102. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Sensitive Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

103. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

104. Defendant has admitted that the Sensitive Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

105. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

106. And, on information and belief, Plaintiff's Sensitive Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

107. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

108. Plaintiff realleges all previous paragraphs as if fully set forth below.

109. Plaintiff and the Class delivered their Sensitive Information to Defendant as part of the process of obtaining treatment and services provided by Defendant.

110. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

111. In providing their Sensitive Information, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

112. In delivering their Sensitive Information to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

113. Plaintiff and the Class Members would not have entrusted their Sensitive Information to Defendant in the absence of such an implied contract.

114. Defendant accepted possession of Plaintiff's and Class Members' Sensitive Information.

115. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure patients' Sensitive Information, Plaintiff and members of the Class would not have provided their Sensitive Information to Defendant.

116. Defendant recognized that patients' Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

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

118. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

119. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

120. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

121. Plaintiff realleges all previous paragraphs as if fully set forth below.

122. This claim is pleaded in the alternative to the breach of implied contract claim.

123. Plaintiff and members of the Class conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

124. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods it sold to Plaintiff and the Class.

125. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class's Sensitive Information because Defendant failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information to Defendant had they known Defendant would not adequately protect their Sensitive Information.

126. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

127. Plaintiff realleges all previous paragraphs as if fully set forth below.

128. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Sensitive Information; (2) to timely notify Plaintiff and Class Members of a

Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

129. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its, in particular, to keep secure their Sensitive Information.

130. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

131. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Sensitive Information.

132. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

133. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Sensitive Information.

134. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their

Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

135. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

PRAYER FOR RELIEF

Plaintiff demands a jury trial for all claims so triable.

Dated: October 28, 2026

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Griffith B. Bludworth (0104784)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com
gbludworth@msdlegal.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and Proposed Class