UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

ROBERTA LINDENBAUM, individually and on behalf of all others similarly situated, Plaintiff, v. UNIVERSITY HOSPITALS HEALTH SYSTEM, INC. d/b/a UNIVERSITY HOSPITALS, Defendant.	Case No. 1:26-cv-2868 **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Roberta Lindenbaum ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendant University Hospitals Health System, Inc. d/b/a University Hospitals ("University Hospitals" or "Defendant"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against University Hospitals for its failure to secure and safeguard the personally identifiable information ("PII") and personal health information ("PHI") of its current and former patients (including Plaintiff).

2. University Hospitals is a health system that operates throughout northern Ohio.

3. On or about October 22, 2026, an unauthorized third party gained access to University Hospitals' network systems containing the PII/PHI of University Hospitals' current and former patients, including Plaintiff (the "Data Breach").

4. University Hospitals owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. University Hospitals breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its current and former patients' PII/PHI from unauthorized access and disclosure.

5. As a result of University Hospitals' inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Roberta Lindenbaum

7. Plaintiff Roberta Lindenbaum is a citizen of Cuyahoga County, Ohio.

8. Plaintiff is a current patient of University Hospitals. As a condition of providing services to Plaintiff, University Hospitals required Plaintiff to provide it with her PII/PHI.

9. Plaintiff believed University Hospitals had implemented and maintained reasonable security practices to protect her PII/PHI. With this belief in mind, Plaintiff provided her PII/PHI to University Hospitals in connection with obtaining services from University Hospitals.

10. At all relevant times, University Hospitals stored and maintained Plaintiff's PII/PHI on its network systems. On information and belief, this includes the systems accessed in the Data Breach.

11. Had Plaintiff known that University Hospitals does not adequately protect the PII/PHI in its possession, she would not have obtained services from University Hospitals or agreed to entrust it with her PII/PHI.

12. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantially increased and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; deprivation of the value of her PII/PHI; lost time mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Defendant University Hospitals Health System, Inc. d/b/a University Hospitals

13. Defendant University Hospitals Health System, Inc. d/b/a University Hospitals is an Ohio non-profit corporation with its principal place of business located at 3605 Warrensville Center Road, Shaker Heights, Ohio 44122. University Hospitals can be served through its registered agent, C T Corporation System, 4400 Easton Commons, Suite 125, Columbus, Ohio 43219.

JURISDICTION AND VENUE

14. The Court has subject matter 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, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

15. This Court has personal jurisdiction over Defendant because it is incorporated in and has its principal place of business in Ohio.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Defendant's principal place of business is in this District and a significant amount of the events leading to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of University Hospitals and the Data Breach

17. University Hospitals is a large health system in northern Ohio with "21 hospitals (including five joint ventures), more than 50 health centers and outpatient facilities, and over 200 physician offices in 16 counties."[1]

18. In the regular course of its business, University Hospitals collects and maintains the PII/PHI of its current and former patients. University Hospitals required Plaintiff and Class members to provide it with their PII/PHI as a condition of providing them with healthcare services.

19. University Hospitals' website contains a HIPAA Notice of Privacy Policies (the "Privacy Policy") describing how University Hospitals may use and disclose patients' PII/PHI.[2] University Hospitals represents that it is "committed to protecting your medical information."[3]

20. The Privacy Policy identifies circumstances in which University Hospitals may disclose patients' medical information without their written authorization. None of these include allowing unauthorized persons to access University Hospitals' systems.[4]

---

[1] *About University Hospitals*, UNIVERSITY HOSPITALS, https://www.uhhospitals.org/about-uh (last accessed Oct. 30, 2026).
[2] *HIPAA Notice of Privacy Policies*, UNIVERSITY HOSPITALS, https://www.uhhospitals.org/patients-and-visitors/hipaa-notice-of-privacy-practices (last accessed Oct. 30, 2026).
[3] *Id.*
[4] *Id.*

21. Plaintiff and Class members are current or former patients of University Hospitals who entrusted University Hospitals with their PII/PHI.

22. On or about October 22, 2026, University Hospitals "detected unusual activity on University Hospitals servers."[5] As a result, University Hospitals "disconnected [its] systems from the internet," implying that an unauthorized third party had gained access.[6] Most of its websites remained down a week after the Data Breach occurred.[7]

23. On information and belief, University Hospitals has not yet notified persons whose PII/PHI was impacted in the Data Breach that their PII/PHI was impacted.

Defendant Knew that Criminals Target PII/PHI

24. At all relevant times, University Hospitals knew, or should have known, that the PII/PHI that it collected and stored was a target for malicious actors. Despite such knowledge, University Hospitals failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyberattacks that it should have anticipated and guarded against.

25. It is well known among companies that store sensitive PII/PHI that such information is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[8]

---

[5] *Cybersecurity Incident*, UNIVERSITY HOSPITALS, https://www.uhhospitals.org/cybersecurity-incident (last accessed Oct. 30, 2026).
[6] *Id*.
[7] Ida Lieszkovsky, *Most University Hospitals Websites Still Down a Week After Cybersecurity Incident*, IDEASTREAM PUBLIC MEDIA (Oct. 29, 2026, 12:58 PM EDT), https://www.ideastream.org/health/2026-10-29/most-university-hospitals-websites-still-down-a-week-after-cybersecurity-incident.
[8] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies*

26. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2025 report, Kroll found that "the healthcare industry was the most breached" in 2024.[9] The company found that 23% of the breaches that it handled responses for were from the healthcare industry, up from 18% in 2023.[10]

27. PII/PHI is a valuable property right.[11] The value of PII/PHI as a commodity is measurable.[12] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black market," or the "dark web," for many years.

28. Criminals piece together bits and pieces of compromised PII/PHI for profit by creating "Fullz" packages. "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security

---

recently, your data may have been stolen, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[9] *Data Breach Outlook*, KROLL, https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2025 (last accessed Oct. 30, 2026).

[10] *See id*.

[11] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[12] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[13] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[14] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

number, date of birth, and more.

29. With "Fullz" packages, cybercriminals can cross-reference two sources of PII/PHI to marry unregulated data available elsewhere with criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

30. The development of "Fullz" packages means that the PII/PHI from the Data Breach can easily be used to link it to Plaintiff's and Class members' 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 PII/PHI that was accessed in the Data Breach, criminals may still 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.

31. Thus, even if certain information (such as contact information) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to criminals.

32. As a result of the real and significant value of these data, identity thieves and other cybercriminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

33. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[15] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[16]

34. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[18]

35. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[19] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[20]

---

[15] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[16] *Id.*

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

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

[19] Steager, *supra* note 15.

[20] *Id.*

36. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[21]

37. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

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

38. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[22] [23]

39. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying

[21] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[22] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Oct. 30, 2026).

[23] The Consumer Financial Protection Bureau defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The Consumer Financial Protection Bureau 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." 12 C.F.R. § 1022.3(g).

for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[24]

40. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[25]

41. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[26] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[27] In warning consumers about the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [28] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[29]

---

[24] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[25] Identity Theft Resource Center, *2025 Consumer Impact Report*, IDENTITY THEFT RES. CTR. (2025), https://www.idtheftcenter.org/publication/itrc-2025-consumer-impact-report/ (last accessed Oct. 30, 2026).

[26] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[27] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 18.

[28] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Oct. 30, 2026).

[29] *Id*.

42. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[30]

43. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[31]

[30] *See* Dixon & Emerson, *supra* note 26.

[31] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

44. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was specifically targeted and taken by someone intending to use that information for any number of improper purposes, including fraud and scams, and making the information available for sale on the black market.

Damages Sustained by Plaintiff and Class Members

45. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in University Hospitals' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

46. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

47. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

> All persons whose personally identifiable information and personal health information were accessed and disclosed in the Data Breach to unauthorized persons.

48. Excluded from the Class are University Hospitals Health System, Inc. d/b/a University Hospitals, and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge.

49. 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 alleging the same claims.

50. The members of the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. While University Hospitals has not reported the number of Class members affected, University Hospitals maintains 21 hospitals and many other medical facilities.[32] The company estimates that it provides care to "more than a million patients per year."[33]

51. Common questions of law or fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant had a duty not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. Whether an implied contract existed between Class members and Defendant, providing that Defendant would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. Whether Defendant breached its duties to protect Plaintiff's and Class members' PII/PHI; and

f. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

[32] *See About University Hospitals*, *supra* note 1.
[33] *Id*.

52. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

53. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

54. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

55. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management

difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

56. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

57. University Hospitals owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in its possession, custody, or control.

58. University Hospitals knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. University Hospitals knew or should have known of the many data breaches that targeted healthcare providers that collect and store PII/PHI in recent years.

59. Given the nature of University Hospitals' business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, University Hospitals should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

60. University Hospitals breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

61. It was reasonably foreseeable to University Hospitals that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data

security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

62. But for University Hospitals' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

63. As a result of University Hospitals' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in University Hospitals' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

64. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

65. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of

Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

66. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

67. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

68. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

69. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

70. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

71. It was, or should have been, reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and

software and hardware systems would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

72. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in University Hospitals' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

73. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

74. Plaintiff and Class members gave University Hospitals their PII/PHI in confidence, believing that University Hospitals would protect that information. Plaintiff and Class members would not have provided University Hospitals with this information had they known it would not be adequately protected. University Hospitals' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between University Hospitals and Plaintiff and Class members. In light of this relationship, University Hospitals

must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

75. Due to the nature of the relationship between University Hospitals and Plaintiff and Class members, Plaintiff and Class members were entirely reliant upon University Hospitals to ensure that their PII/PHI was adequately protected. Plaintiff and Class members had no way of verifying or influencing the nature and extent of University Hospitals' data security policies and practices, and University Hospitals was in an exclusive position to guard against the Data Breach.

76. University Hospitals has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

77. As a direct and proximate result of University Hospitals' breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in University Hospitals' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with University Hospitals.

80. Pursuant to these implied contracts, Plaintiff and Class members paid money to University Hospitals, directly or through their insurance, and provided University Hospitals with their PII/PHI. In exchange, University Hospitals agreed to, among other things, and Plaintiff and Class members understood that University Hospitals would: (1) provide healthcare services to Plaintiff and Class members; (2) collect, maintain, and utilize Plaintiff's and Class members' PII/PHI to, among other things, facilitate their treatment and the provision of healthcare services to Plaintiff and Class members; (3) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; (4) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations, industry standards, and University Hospitals' representations; and (5) maintain the confidentiality of Plaintiff's and Class members' PII/PHI and protect it from unauthorized access, disclosure, theft, and misuse.

81. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and University Hospitals, on the other hand. Had Plaintiff and Class members known that University Hospitals would not adequately protect its patients' PII/PHI, they would not have agreed to provide University Hospitals with their PII/PHI and would not have received healthcare services from University Hospitals.

82. Plaintiff and Class members performed their obligations under the implied contract when they provided University Hospitals with their PII/PHI and paid—directly or through their insurers—for healthcare services from University Hospitals.

83. University Hospitals breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain reasonable security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, industry standards, and University Hospitals' representations.

84. University Hospitals' breach of its obligations under its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

85. Plaintiff and all other Class members were damaged by University Hospitals' breach of implied contracts because: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in University Hospitals' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

86. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

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

88. Plaintiff and Class members conferred a monetary benefit upon University Hospitals in the form of monies paid for healthcare services and through the provision of their PII/PHI.

89. University Hospitals accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. University Hospitals also benefited from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate its operations and billing services.

90. As a result of University Hospitals' conduct, University Hospitals' current and former patients suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that patients paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

91. University Hospitals should not be permitted to retain the money belonging to Plaintiff and Class members because University Hospitals failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for expecting and that were otherwise mandated by federal, state, and local laws and industry standards.

92. Plaintiff and Class members have no adequate remedy at law.

93. University Hospitals should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable under law;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: October 30, 2026

Respectfully submitted,

/s/
Adam T. Savett
WOLF POPPER LLP
570 Lexington Ave.
New York, NY 10022
Tel: 212-759-4600
ASavett@wolfpopper.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Counsel for Plaintiff

**pro hac vice forthcoming*