UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

PATRICK NOLAN, individually and on behalf of all others similarly situated, Plaintiff, v. ANN & ROBERT H. LURIE CHILDREN'S HOSPITAL OF CHICAGO, Defendant.	Case No.: 1:24-cv-05901 JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Patrick Nolan ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his attorneys, brings this action against the Ann & Robert H. Lurie Children's Hospital of Chicago ("Defendant") and alleges, upon his personal knowledge and as to his own actions and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Patients entrust hospitals with their most sensitive personal and medical information, including their names, dates of birth, Social Security numbers, health history, medical conditions, medications, demographics, and family health history. They do so with the understanding that hospitals will protect this information and guard against its misuse.

2. Defendant is a nationally ranked pediatric acute care children's hospital located in Chicago, Illinois and touts itself as the largest pediatric provider in the region. As such, Defendant's everyday course of business requires the gathering of highly sensitive personally

identifiable information ("PII") such as name, address, date of birth, dates of service, driver's license, email address, telephone number, and Social Security number, as well as personal health information ("PHI") including health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, and prescription information. Defendant regularly collects PII and PHI information from children.

3. Yet Defendant failed to properly protect the PII and PHI it collects, including that of its minor patients, by investing in adequate data security, thereby allowing hackers to exfiltrate the highly sensitive PII and PHI entrusted to Defendant. Between January 26 and 31, 2024, at least one unauthorized third party accessed the data of at least 791,784 patients (the "Data Breach") during a cyber-attack that required Defendant to take certain electronic systems offline "to protect [its] systems and [its] ability to continue operations."[1]

4. The compromised data included minor patients' and other individuals' names, addresses, dates of birth, dates of service, driver's license numbers, email addresses, health claims information, health plans, health plan beneficiary numbers, medical conditions or diagnoses, medical record numbers, medical treatments, prescription information, Social Security numbers, and telephone numbers.

5. After the January 2024 cyber-attack, reports circulated online as early as March 2024 that stolen patient data was sold on the dark web for $3.4 million.[2] Nearly five months after the data was compromised, Defendant discovered the Data Breach on June 17, 2024.

6. While Defendant has not outright stated that the attack was a ransomware attack, the details revealed about the cyber-attack bear all the hallmarks of a ransomware attack, which is

[1] https://www.luriechildrens.org/en/lurie-childrens-notifies-individuals-of-data-breach/.

[2] https://www.beckershospitalreview.com/cybersecurity/hackers-say-they-sold-lurie-childrens-hospital-data-for-3-4m.html (last accessed July 10, 2024).

a type of cyberattack in which the attackers encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[3] According to Defendant, "Lurie Children's did not pay a ransom."[4]

7. Despite Defendant's statement that it "take[s] seriously the privacy of our patients' and team members' sensitive information,"[5] Defendant inexplicably failed to implement and maintain reasonable and adequate security procedures and practices to safeguard the PII and PHI of Plaintiff and the Class. Despite the more than five months that have passed since the cyber-attack, Defendant justifies its delayed response with nothing more than the cursory statement that "it has taken time to understand what happened and to identify the scope of impact to our systems and data."[6]

8. The size of the Data Breach and information Defendant has disclosed about the breach to date, including the sensitive nature of the impacted data and the time it took for Defendant to identify the breach, collectively demonstrate Defendant failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive patient information.

9. Defendant knew or should have known of the serious risk of harm caused by a data breach, including the importance of acting swiftly to protect PII and PHI. Yet, Defendant ignored reports of the Data Breach and black-market data sale as early as March 2024, only confirmed the

[3] https://www.varonis.com/blog/what-is-ransomware (last accessed July 10, 2024).
[4] https://www.luriechildrens.org/en/lurie-childrens-notifies-individuals-of-data-breach/ (last accessed July 10, 2024).
[5] *Id.*
[6] *Id.*

Data Breach on June 17, 2024, and waited more than ten days after that to disclose the breach on June 27, 2024.[7]

10. Defendant's failure to promptly recognize and notify Plaintiff and Class members that their PII and/or PHI was implicated due to Defendant's security failures virtually ensured that the unauthorized third parties who exploited Defendant's security vulnerabilities could monetize, misuse, and/or disseminate that PII and PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated even beyond the Data Breach itself.

11. Plaintiff and Class members had a reasonable expectation and understanding that Defendant would adopt adequate data security safeguards to protect their PII and PHI.

12. However, Defendant failed to: take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data to prevent the Data Breach from occurring; disclose to patients and individuals providing PII and PHI the material fact that it lacked appropriate data systems and security practices to secure PII and PHI; and timely detect and provide adequate notice of the Data Breach to affected individuals. Because of Defendant's failures, Plaintiff and Class members suffered substantial harm and injury.

13. As a direct result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its obligations, Plaintiff's and Class members' PII and PHI was accessed and acquired by unauthorized third parties for the purpose of misusing the data

[7] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/64c3b313-0c3c-4820-af10-6afef36d08e1.html (last accessed July 10, 2024).

and causing further irreparable harm to the personal, financial, medical, and future well-being of patients and individuals who provided Defendant with their PII and PHI.

14. Plaintiff and Class members face the real, immediate, and likely danger of identity theft and misuse of their PII and PHI, especially because their PII and PHI was specifically targeted by malevolent actors. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

15. Plaintiff and Class members suffered injuries as a result of Defendant's conduct, including, but not limited to: loss of privacy in their PHI; lost or diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to, the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and the continued and increased risk of compromise to their PII, 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 PII and PHI it collects. These risks will remain for the lifetimes of Plaintiff and the Class.

16. Plaintiff brings this action individually and on behalf of the Class, seeking relief including, but not limited to, actual damages, punitive damages, restitution, statutory damages, injunctive relief, and a declaratory judgment, reasonable attorneys' fees and costs, and all other remedies this Court deems proper.

II. PARTIES

17. Plaintiff Patrick Nolan has been at all relevant times a citizen and resident of the State of Illinois.

18. Defendant Ann & Robert H. Lurie Children's Hospital of Chicago is a Chicago-based, Illinois pediatric healthcare provider with a principal place of business located at 225 E. Chicago Ave., Chicago, Illinois 60611. Defendant maintains more than 54 locations throughout Illinois and the Chicagoland area.

III. JURISDICTION

19. 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 costs and interest. At least one member of the Class is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

20. Venue is proper in this judicial district under 28 U.S.C. § 1391 because Defendant maintains a principal place of business in this district, and because a substantial portion of the events giving rise to Plaintiff's claims occurred here.

21. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Chicago, Illinois.

IV. FACTUAL BACKGROUND

A. Background

22. Defendant is one of the largest pediatric hospitals in the Midwest. Besides the main hospital in downtown Chicago, Defendant maintains more than 50 Lurie's facilities throughout the Chicagoland area.[8]

23. Defendant employes more than 1,800 physicians and health professionals and treats approximately 239,000 children per year.[9]

[8] https://www.luriechildrens.org/en/locations/ (last accessed July 10, 2024).
[9] https://www.luriechildrens.org/en/who-we-are/facts-figures/ (last accessed July 10, 2024).

24. As part of its regular business operations, Defendant collected and stored PII and PHI such as name, address, date of birth, dates of service, driver's license, email address, telephone number, and Social Security number, health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, and prescription information.

25. Defendant was entrusted with and obligated to safeguard and protect PII and PHI of Plaintiff and the Class in accordance with all applicable laws and industry standards.

26. In fact, Defendant promises patients it "believes in protecting the privacy of your health information" in its Privacy Policy available on its website.[10] While acknowledging that it collects PII and PHI, Defendant admits that it is "required by law to . . . assure that patient information that identifies you is kept confidential in accordance with law."[11] Furthermore, Defendant states that it "must obtain your written authorization to use or disclose your patient information."[12]

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' sensitive information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from unauthorized disclosure.

B. The Data Breach

28. Beginning on June 27, 2024, Defendant began notifying victims of a data breach that occurred between January 26 and 31, 2024. The January cyber-attack caused Defendant to

[10] https://www.luriechildrens.org/en/privacy-legal-information/notice-of-privacy-practices/ (last accessed July 10, 2024).
[11] *Id*.
[12] *Id*.

take some of its electronic systems offline, including email, phones, its electronic health record system (Epic), and the patient portal (MyChart).[13]

29. More than five months after the cyber-attack, Defendant determined that the Data Breach impacted the following PII and PHI: name, address, date of birth, dates of service, driver's license number, email address, health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, prescription information, Social Security number, and telephone number.[14]

30. Defendant's failure to promptly notify Plaintiff and Class members that their PII and PHI was implicated due to Defendant's security failures put Plaintiff and the Class at further risk because their information was vulnerable for more than five months without their knowledge. Plaintiff and the Class were not able to take affirmative actions to protect their identity or watch for consequences of malicious misuse of their PII and PHI.

31. Despite Defendant's lengthy five month long investigation, its Data Breach notification fails to provide critical information as to how the Data Breach occurred, who or what accessed PII and PHI, how Defendant failed to detect the Data Breach, and why it took so long for Defendant to determine the Data Breach occurred and its scale.

C. Defendant's Failures Prior to and Following the Data Breach

32. Defendant has an obligation to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and Class members' PII. Defendant's obligations are derived from: 1) government regulations and laws, including FTC rules and regulations and the Health

[13] https://www.luriechildrens.org/en/lurie-childrens-notifies-individuals-of-data-breach/ (last accessed July 10, 2024).

[14] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/64c3b313-0c3c-4820-af10-6afef36d08e1.html (last accessed July 10, 2024).

Insurance Portability and Accountability Act ("HIPAA"); 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII. Plaintiff and Class members provided—and Defendant obtained—their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

33. Defendant knew it was storing sensitive PII and PHI and that, as a result, its systems would be an attractive target for cybercriminals.

34. Cyber-attacks and ransomware attacks are frequently used to target companies or large entities due to the volume of sensitive data that they collect, maintain, and store.[15] From 2022 to 2023, statistics show more than a 73% increase[16] in ransomware attacks, resulting in more than $1.1 billion in ransomware payments.[17]

35. According to the Center for Internet Security, companies should treat ransomware attacks as any other data breach incident because ransomware attacks do not simply hold networks hostage and/or publicly disclose the data; rather, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[18]

36. Defendant could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and network files containing PII and PHI.

---

[15] Charles Griffiths, *The Latest 2023 Cyber Crime Statistics (updated October 2023)*, AAG (Feb. 10, 2023), available at https://aag-it.com/the-latest-cyber-crime-statistics/ (last accessed July 11, 2024).

[16] https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/ (last accessed July 11, 2024).

[17] https://www.chainalysis.com/blog/ransomware-2024/ (last accessed July 11, 2024).

[18] *Ransomware: The Data Exfiltration and Double Extortion Trends*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last accessed July 11, 2024).

37. Despite widespread industry warnings, Defendant failed to implement and use reasonable security procedures and practices to protect Plaintiff's and similarly situated individuals' sensitive PII and PHI.

38. Defendant's failure to properly safeguard Plaintiff's and Class members' PII and PHI allowed unauthorized actors to access sensitive PII and PHI.

39. The Data Breach highlights the inadequacies inherent in Defendant's network monitoring procedures and security training protocols. If Defendant had properly monitored its cybersecurity systems and implemented a sufficient training protocol for its employees, it would have prevented the Data Breach, detected the Data Breach sooner, and/or have prevented the hackers from accessing PII and PHI.

40. Moreover, Defendant has not yet informed affected individuals of the length of time that the unauthorized actors had access to their PII and PHI, when the breach occurred, or the full extent of the PII and PHI that was accessed during the Data Breach.

41. Defendant's failure to timely notify Plaintiff and other victims of the Data Breach that their PII and PHI had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII and PHI.

42. Defendant's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

43. Defendant's failures are three-fold. First, Defendant failed to timely secure its computer systems to protect patients' and staffs' PII and PHI. Defendant allowed unauthorized actors to access the records of nearly 800,000 patients and other individuals without detection. As a result, Plaintiff's and the Class's PII and PHI was allegedly sold on the dark web.[19]

[19] https://www.beckershospitalreview.com/cybersecurity/hackers-say-they-sold-lurie-childrens-

44. Second, Defendant failed to timely notify affected individuals, including Plaintiff and Class members, that their highly sensitive PII and PHI had been accessed by unauthorized third parties. Although reports circulated online about the Data Breach as early as March 2024, Defendant failed to take any action until June 27, 2024.

45. Third, Defendant made no effort to protect Plaintiff and the Class from the long-term consequences of Defendant's acts and omissions. Although Defendant offered victims 24 months of credit monitoring, Plaintiff's and Class members' PII and PHI, including their Social Security numbers, cannot be changed and will remain at risk long into the future. As a result, Plaintiff and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

46. In short, Defendant's myriad failures, including the failure to timely detect the Data Breach and to notify Plaintiff and the Class with reasonable timeliness that their PII had been accessed due to Defendant's security failures, allowed unauthorized individuals to access and misappropriate Plaintiff's and Class members' PII and PHI for an unknown amount of time before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

47. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors and lead to considerable costs to consumers. According to Statista, during the first quarter of 2023 alone, more than six million data records were exposed

hospital-data-for-3-4m.html (last accessed July 11, 2024).

worldwide through data breaches.[20] Indeed, cybercrime is slated to cost the world $10.5 trillion annually by 2025.[21]

48. Identity theft is the most common consequence of data breaches to consumers. A 2021 report concluded that more than half of all data breaches resulted in identity theft, including unauthorized access to a victim's financial accounts, opening new accounts in the victim's name, and using a victim's personal information for other fraudulent activities.[22]

49. As a result, PII is an invaluable commodity and the most frequent target of hackers.[23] Numerous sources cite dark web pricing for personal information, such as name, date of birth, and Social Security number, ranging from $40 to $200.[24]

50. Many tend to minimize the value of certain categories of PII, such as names, birthdates, addresses, and phone numbers. However, security experts agree that "[i]f you have someone's name and address, that is still valuable."[25] At the end of the day, "the more info you have, the more it is worth."[26]

---

[20] https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ (last accessed July 11, 2024).

[21] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, Cybercrime Magazine (Nov. 13, 2020), available at https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (last accessed July 11, 2024).

[22] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 11, 2024).

[23] *Id*.

[24] *Id*.

[25] Robert Lemos, *All about your 'fullz' and how hackers turn your personal data into dollars*, PCWorld (June 2, 2016), available at https://www.pcworld.com/article/414992/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html (last accessed July 11, 2024).

[26] *Id.*

51. Thefts of Social Security numbers present an even greater risk to consumers. Indeed, data breaches involving Social Security numbers are "incredibly alarming" because "[u]nlike a credit card number which can be changed, Social Security numbers . . . are hard to change, or cannot be changed."[27]

52. Even if victims whose Social Security numbers have been compromised are able to change their Social Security numbers, the new number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

53. According to the FTC, in 2021, around 20% of Americans were victims of identity theft, indicating that most Americans have either been a victim of identity theft or know someone who has.[29]

54. The fraudulent activity resulting from Defendant's Data Breach may not come to light for years, as there may be a time lag between when Plaintiff's and Class members' PII was stolen and when it is used, meaning there may be a delay between when the harm occurs versus when it is discovered.[30]

---

[27] Brian Naylor, *Victims Of Social Security Number Theft Find It's Hard To Bounce Back*, NPR (Feb. 9, 2015), available at https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed July 11, 2024).

[28] *Id*.

[29] *Consumer Sentinel Network Data Book 2021*, Federal Trade Commission (Feb. 2022), available at https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (last accessed July 11, 2024).

[30] *Report to Congressional Requesters*, Government Accountability Office, at 29 (June 2007), available at https://www.gao.gov/assets/gao-07-737.pdf (last accessed July 11, 2024).

55. Beyond economic impacts, identity theft also leads to lasting emotional impacts; a majority of the victims of identity theft report increased stress levels, fatigue, and trust issues with family and friends and decreased energy.[31]

56. Cyber-attacks against hospitals are often carried out to exfiltrate PHI that can be used for Medicare or other medical fraud.[32]

57. Despite the prevalence of public announcements of data breach and data security compromises and the risks posed by compromises of PII and PHI, Defendant failed to take proper action to protect the PII of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its patients and staff.

E. Defendant's Conduct Violated FTC Guidelines, HIPAA, and Industry Standards for Safeguarding Patients' PII and PHI

58. The FTC rules, regulations, and guidelines as well as HIPAA and industry standards obligate organizations like Defendant to protect PII from unauthorized access or disclosure by unauthorized persons.

59. At all relevant times, Defendant was fully aware of its obligation to protect PII and PHI because it is a sophisticated business entity that is in the business of maintaining and transmitting PII and PHI.

---

[31] *New Study by Identity Theft Resource Center Explores the Non-Economic Negative Impacts Caused by Identity Theft*, Identity Theft Resource Center (Oct. 18, 2018), available at https://www.idtheftcenter.org/post/new-study-by-identity-theft-resource-center-explores-the-non-economic-negative-impacts-caused-by-identity-theft/#:~:text=Due%20to%20their%20identity%20theft,at%20school%20(eight%20percent) (last accessed July 11, 2024).

[32] https://www.techtarget.com/searchhealthit/definition/PHI-breach-protected-health-information-breach (last accessed July 11, 2024).

60. Defendant was also aware of the significant consequences of its failure to protect PII and PHI, and knew that this data, if hacked, would injure individuals, including Plaintiff and Class members.

61. Defendant failed to comply with Federal Trade Commission ("FTC") rules, regulations, and guidelines and industry standards concerning the protection and security of PII. Defendant has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

62. Defendant is subject to the requirements of HIPAA. As a regular and necessary part of its business, Defendant collects and stores the highly sensitive PHI of patients and other individuals. Defendant is required under federal law to maintain the strictest confidentiality of the PHI that it acquires, receives, and collects.

63. Specifically, Defendant has a duty to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

64. As evidenced by the unknown duration, scope, and nature of the Data Breach, among its many deficient practices, Defendant failed in, *inter alia*, the following industry standard best practices:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

d. Ensuring the confidentiality and integrity of PII and PHI collected from patients and others;

e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of PII and PHI collected from patients and others;

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Implementing technical policies, procedures, and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of PII and PHI collected by Defendant.

65. Defendant is subject to the requirements of HIPAA. As a regular and necessary part of its business, Defendant collects and stores the highly sensitive PHI of patients and other individuals. Defendant is required under federal law to maintain the strictest confidentiality of the patients' PHI that it acquires, receives, and collects.

66. Specifically, Defendant has a duty to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health

information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

67. Had Defendant implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendant could have prevented or detected the Data Breach prior to the hackers accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and patients and impacted individuals would have been notified sooner, allowing them to promptly take protective and mitigating actions.

F. Plaintiff's Experience

68. In early July 2024, Plaintiff became aware he was implicated in the Data Breach.

69. On July 11, 2024, Plaintiff contacted Defendant's Data Breach call center and confirmed that his information had been implicated in the Data Breach.

70. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; monitoring his accounts and credit; and taking other steps to protect against the use of his PII. Plaintiff has spent valuable time dealing with the Data Breach, time Plaintiff otherwise would have spent on other activities, including work and/or recreation.

71. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights;

(c) present, imminent, and impending injury arising from the increased risk of identity theft; and (d) loss of benefit of the bargain.

72. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

73. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class defined as:

> **All persons in the United States whose PII was accessed in the Data Breach announced by Defendant on June 27, 2024 (the "Class").**

74. Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the Class definition after conducting discovery.

75. In addition, Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), an Illinois Subclass defined as:

> **All persons who are residents of the State of Illinois whose PII was accessed in the Data Breach announced by Defendant on June 27, 2024 (the "Illinois Subclass").**

76. Excluded from the Illinois Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

77. The Nationwide Class and the Illinois Subclass are collectively referred to herein as the "Class."

78. **Numerosity**: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that at least 791,784 individuals were affected by the Data Breach. The members of the Class will be identified through information and records in Defendant's possession, custody, and control.

79. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Defendant's data security and retention policies were unreasonable;

b. Whether Defendant failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII and PHI;

d. Whether Defendant breached any legal duties in connection with the Data Breach;

e. Whether Defendant's conduct was intentional, reckless, willful, or negligent;

f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII and PHI;

g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and PHI and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

h. Whether Plaintiff and Class members suffered damages as a result of Defendant's conduct; and

i. Whether Plaintiff and the Class are entitled to monetary damages, injunctive relief, and/or other remedies and, if so, the nature of any such relief.

80. **Typicality**: Plaintiff's claims are typical of the claims of the Class because Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The actions and omissions that gave rise to Plaintiff's claims are the same that gave rise to the claims of every other Class member because Plaintiff and each Class member had their sensitive PII and/ or PHI compromised in the Data Breach due to Defendant's misconduct, and there are no defenses that are unique to Plaintiff.

81. **Adequacy**: Plaintiff is an adequate representative because his interests do not conflict with the interests of the Class that he seeks to represent, he retained counsel competent and highly experienced in complex class action litigation, and he intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

82. **Superiority**: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties,

and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based on Defendant's records.

83. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE

(On Behalf of Plaintiff and the Class)

84. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

85. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII and PHI that Defendant collected.

86. Defendant owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII and PHI that Defendant collected.

87. Defendant owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is and was discovered.

88. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

89. Defendant solicited, gathered, and stored the PII and PHI belonging to Plaintiff and the Class.

90. Defendant knew or should have known it inadequately safeguarded this information.

91. Defendant knew that a breach of its systems would inflict harm and damages upon Plaintiff and Class members, and Defendant was therefore charged with a duty to adequately protect this critically sensitive information.

92. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' highly sensitive PII and PHI was entrusted to Defendant on the understanding that adequate security precautions would be taken to protect the PII and PHI. Moreover, only Defendant had the ability to protect its systems and the PII and PHI stored on them from attack.

93. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff, Class members, and their PII and PHI. Defendant's misconduct included failing to: (1) secure its systems, servers, and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement safeguards, policies, and procedures necessary to prevent this type of data breach.

94. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII and PHI belonging to Plaintiff and the Class.

95. Defendant breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

96. Defendant breached the duties it owed to Plaintiff and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII and PHI.

97. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII and PHI belonging to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII and PHI.

98. Defendant breached the duties it owed to Plaintiff and the Class by failing to disclose timely and accurately to Plaintiff and Class members that their PII and PHI had been improperly acquired or accessed.

99. Defendant breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until on or about June 27, 2024.

100. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to, time and expenses incurred in mitigating the effects of the Data Breach.

101. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Class)

102. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

103. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

104. Pursuant to HIPAA, Defendant has duty to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

105. Defendant violated the FTC rules and regulations and HIPAA obligations that require companies to use reasonable measures to protect PII and PHI. Specifically, Defendant failed to comply with applicable security standards and unduly delayed reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, the foreseeable consequences of the Data Breach, and the exposure of Plaintiff's and Class members' sensitive PII and PHI.

106. Defendant's violations of the FTC rules and HIPAA constitute negligence *per se*.

107. Plaintiff and the Class are within the category of persons the FTC Act was intended to protect.

108. Plaintiff and the Class are within the category of persons HIPAA was intended to protect.

109. The harm that occurred as a result of the Data Breach described herein is the type of harm the FTC Act was intended to guard against.

110. The harm that occurred as a result of the Data Breach described herein is the type of harm HIPAA was intended to guard against.

111. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII and PHI in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III- BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Class)

112. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

113. When Plaintiff and Class members provided their PII and PHI to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to adopt reasonable safeguards complying with relevant laws, regulations, and industry practices, including HIPPA, to protect their PII and PHI, and to timely notify them in the event of a data breach.

114. Defendant solicited and invited Plaintiff and Class members to provide their PII and PHI as a condition of Defendant's provision of healthcare or other services. Plaintiff and Class members accepted Defendant's offers and provided their PII and PHI to Defendant.

115. When entering implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant would implement reasonable data security measures and that Defendant's data security practices complied with relevant laws, regulations, and industry standards. Defendant knew or should have known that Plaintiff and Class members held this belief and expectation.

116. Implicit in the agreement between Plaintiff and Class members and Defendant was Defendant's obligation to: (a) adequately safeguard Plaintiff's and Class members' PII and PHI; (b) prevent unauthorized access and/or disclosure of Plaintiff's and Class members' PII and PHI; (c) provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII and PHI; and (d) retain Plaintiff's and Class members' PII and PHI under conditions that kept such information secure and confidential.

117. Defendant's conduct in requiring patients to provide PII and PHI as a prerequisite to their medical treatment illustrates Defendant's intent to be bound by an implied promise to adopt reasonable data security measures.

118. Plaintiff and Class members would not have provided their PII and PHI to Defendant had they known that Defendant would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

119. Plaintiff and Class members fully and adequately performed their obligations under the implied contracts with Defendant. They provided consideration and their PII and PHI to Defendant in exchange for medical services and Defendant's implied promise to adopt reasonable data security measures.

120. Defendant breached its implied contracts with Plaintiff and Class members by failing to safeguard their PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach.

121. The losses and damages Plaintiff and Class members sustained, include, but are not limited to:

a. Theft of their PII and PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services,

freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members;

j. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

122. The damages sustained by Plaintiff and Class Members were the direct and proximate result of Defendant's material breaches of its agreement(s).

COUNT IV–UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Class)

123. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

124. Plaintiff and Class members conferred benefits upon Defendant. In exchange for providing payment and PII and PHI, Plaintiff and Class members should have received medical treatment or other services accompanied by Defendant's adequate safeguarding of their PII and PHI.

125. Defendant knew that Plaintiff and Class members conferred a benefit on it and accepted, has accepted, or retained that benefit. Defendant profited from Plaintiff's payments and used Plaintiff's and Class members' PII and PHI for business or associate purposes.

126. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead utilized cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over adequate security.

127. Under principles of equity and good conscience, Defendant should not be permitted to retain the full monetary benefit of its transactions with Plaintiff and Class members. Defendant failed to adequately secure PII and PHI and, therefore, did not provide the full services that patient paid for. Class members now must monitor their personal, immutable PII and PHI for the rest of their lives.

128. If Plaintiff and Class members had known that Defendant employed inadequate data security safeguards, they would not have agreed to providing Defendant with PII and PHI.

129. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered the various types of damages alleged herein.

130. Class members have no adequate remedy at law. Defendant continues to retain Class members' PII and PHI, therefore exposing the PII and PHI to a risk of future data breaches in Defendant's possession.

131. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court enter a judgment on their behalf and against Defendant Ann & Robert H. Lurie Children's Hospital of Chicago, and further grant the following relief:

A. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Designate Plaintiff as a representative of the proposed Class and subclass and Plaintiff's counsel as Class counsel;

C. Grant Plaintiff the declaratory relief sought herein;

D. Grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

E. Award Plaintiff and the Class compensatory, consequential, and general damages in an amount to be determined at trial, and any other relief to which they are entitled under the law;

F. Award Plaintiff and the Class statutory damages, and punitive or exemplary damages, to the extent permitted by law;

G. Award prejudgment interest, costs, and attorneys' fees;

H. Award all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. Award Plaintiff and the Class such other and further relief as the Court deems just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the proposed Class, respectfully requests a trial by jury as to all matters so triable.

Dated: July 12, 2024

Respectfully submitted,

By: */s/ Elizabeth A. Fegan*

Elizabeth A. Fegan
Megan E. Shannon
FEGAN SCOTT LLC
150 S. Wacker Drive, 24th Floor
Chicago, IL 60606
Telephone: (312) 741-1019
Facsimile: (312) 264-0100
beth@feganscott.com
megan@feganscott.com