Exhibit A

UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

JOSE A. MORALES ROSARIO, individually and on behalf of all other similarly situated Plaintiff, v. HOSPITAL ESPAÑOL AUXILIO MUTUO DE PUERTO RICO, INC., Defendant.	Case No: 3:25-cv-01244 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, Jose A. Morales Rosario, individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Defendant Hospital Español Auxilio Mutuo de Puerto Rico, Inc. dba Auxilio Mutuo Hospital ("Defendant" or "Auxilio Mutuo Hospital"), alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF THE ACTION

1. This class action arises from Auxilio Mutuo Hospital's failure to protect highly sensitive data. The breach notification posted on Auxilio Mutuo Hospital's website is attached as Exhibit A (the "Breach Notice").[1] The breach notification Auxilio Mutuo Hospital sent Mr. Morales is attached as Exhibit B.

[1] Notificación Sobre Potencial Brecha de Datos, AUXILIO MUTUO, https://www.auxiliomutuo.com/notificacion-sobre-potencial-brecha-de-datos/ (last visited April 30, 2025).

2. Auxilio Mutuo Hospital did not discover on its own that its systems had been compromised, and despite outside expert help and the unreasonably amount of time that has passed, Auxilio Mutuo Hospital claims it is still unable to determine the scope of the Data Breach.

3. According to its Breach Notice, on September 23, 2023, the Department of Homeland Security informed the hospital that its systems were the likely target of a criminal cyber group (the "Data Breach"). Exs. A & B. After launching two investigations, the first concluding on November 21, 2023 and the second concluding on May 15, 2024, Auxilio Mutuo Hospital was able to limit the impacted patients to those who visited the hospital between August 2022 and September 2023. *Id.*

4. On or around April 21, 2025—***575 days after Homeland Security notified Auxilio Mutuo Hospital of the Data Breach***—Auxilio Mutuo Hospital finally began providing written notice of this incident. *Id.*

5. While the information impacted varies depending on the individual, the type of information potentially exposed includes personally identifying information, including names, dates of birth, Social Security numbers, driver's license numbers, state identification numbers, passport numbers, financial and banking information, account numbers, billing codes, payment cards, as well as protected health information including medical information and health insurance information. *Id.* Plaintiff refers to the compromised data as "PII/PHI."

6. While Auxilio Mutuo Hospital does not state how long the Data Breach lasted, its Breach Notice suggests it was massive and lengthy. For an unknown period of time, cybercriminals accessed Auxilio Mutuo Hospital's system undetected, and were able to access patient data from possibly continuing from August 2022 to September 2023, evincing Auxilio Mutuo Hospital's grossly inadequate cybersecurity systems.

7. Moreover, the fact Auxilio Mutuo Hospital waited ***575 days*** from the date of the Homeland Security first notified it of the Data Breach, before it finally began notifying Class Members about the Data Breach, despite the fact that highly sensitive PII/PHI was compromised, evinces gross negligence.

8. Upon information and belief, cybercriminals were able to breach Auxilio Mutuo Hospital's systems because Auxilio Mutuo Hospital failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII/PHI of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI—rendering it an easy target for cybercriminals.

9. The Breach Notice obfuscates the nature of the Data Breach and the threat it posed. Exs. A & B. The Breach Notice fails to disclose how many people were impacted, how the Data Breach happened, how long the Data Breach lasted, how cybercriminals were able to avoid detection for an unknown period of time, how the Department of Homeland Security was able to discover the Data Breach but Auxilio Mutuo Hospital was not, and why it took Auxilio Mutuo Hospital more than 18 months before it finally began notifying some victims that cybercriminals had gained access to their highly private information.

10. Auxilio Mutuo Hospital's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII/PHI.

11. Auxilio Mutuo Hospital knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII/PHI misuse.

12. In failing to adequately protect the PII/PHI of individuals whose PII/PHI was in Auxilio Mutuo Hospital's custody and control, by failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Auxilio Mutuo Hospital violated state law and harmed an unknown number of individuals.

13. Plaintiff and the Class are victims of Auxilio Mutuo Hospital's negligence and inadequate cybersecurity measures. Specifically, Plaintiff and members of the proposed Class trusted Auxilio Mutuo Hospital with their PII/PHI. But Auxilio Mutuo Hospital betrayed that trust when it failed to properly use industry-standard security practices to prevent the Data Breach.

14. Plaintiff is a victim of the Data Breach, having received a Breach Notice on or around April 21, 2025.

15. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

16. Plaintiff seeks, on behalf of himself and the Class, monetary damages and injunctive relief including lifetime credit monitoring and ID theft monitoring.

PARTIES

17. Plaintiff, Jose A. Morales Rosario, is a natural person and citizen of Puerto Rico, residing in Carolina, Puerto Rico, where he intends to remain. Mr. Morales Rosario is a Data Breach victim, receiving Notice of the Data Breach on or around April 21, 2025.

18. Defendant Hospital Español Auxilio Mutuo de Puerto Rico, Inc. dba Auxilio Mutuo Hospital ("Defendant" or "Auxilio Mutuo Hospital"), is a domestic corporation headquartered at Ave Ponce de Leon 715, Parada 37.5, San Juan, Puerto Rico 00918.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over the claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from the Defendants, there are more than 100 putative class members, and the amount in controversy exceeds $5 million.

20. The Court has personal jurisdiction over Defendants because Plaintiff's and Class Members' claims arise out of Defendants' business activities conducted in Puerto Rico, where Defendants' headquarters are located.

21. Venue is appropriate in this District because, among other things: (a) Plaintiff resides in this District, (b) Defendant maintains offices in this District, where it conducts substantial business; (c) Defendant directed its activities at residents in this District; and (d) many of the acts and omissions that give rise to this Action took place in this judicial District.

22. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because Defendant conducts a large amount of their business in this District, and because Defendant has substantial relationships in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiff and the Class

23. Auxilio Mutuo Hospital touts itself as the most comprehensive private hospital in Puerto Rico and the Caribbean, offering first class services and surgical procedures for more than 138 years.[2] Today, Auxilio Mutuo Hospital provides healthcare services in a range of medical areas, including cancer, cardiovascular, surgery, respiratory care, diabetes, dialysis, endoscopy,

[2] About Us, AUXILIO GLOBAL HEALTH, https://www.auxilioglobal.com/about-us.php (last visited April 30, 2025).

nuclear medicine, neurology, nutrition, pediatrics, rehabilitation, and more.[3] Located in San Juan, Puerto Rico, Auxilio Mutuo Hospital employs over 2,000 individuals.[4]

24. Given the nature of the services it provides, Auxilio Mutuo Hospital accumulates highly private PII/PHI of its current and former patients.

25. In collecting and maintaining the PII/PHI of its current and former patients, Auxilio Mutuo Hospital agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII/PHI.

26. Auxilio Mutuo Hospital understood the need to protect the PII/PHI of current and former patients, and the need to prioritize its data security. Indeed, Auxilio Mutuo Hospital represented in the Breach Notice posted on its Website that "We take privacy and security very seriously" (Ex. A) and contains a Privacy Policy purporting to safeguard patient data.[5]

27. On information and belief, Auxilio Mutuo Hospital has not implemented reasonable cybersecurity safeguards or policies to protect the PII/PHI of its employees, clients, and patients, or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to the PII/PHI of its current and former patients.

Defendant Failed to Safeguard the PII/PHI of Plaintiff and the Class

28. Upon information and belief, the Data Breach impacted residents of Puerto Rico, Maryland, New Mexico, New York, North Carolina, Oregon, and Rhode Island. Ex. A.

---

[3] Servicios, AUXILIO MUTUO, https://www.auxiliomutuo.com (last visited April 30, 2025).
[4] *Id.*
[5] *Sign Up and Connect – Patient Portal,* AUXILIO MUTUO, *https://auxiliomutuo.followmyhealth.com/Login/Home/Index?authproviders=0&returnArea=PatientAccess#!/createNew* (last visited April 30, 2025).

29. Plaintiff received a Breach Notice on or around April 21, 2025, indicating his PII/PHI was potentially impacted by the massive and lengthy Data Breach.

30. On information and belief, Defendant collects and maintains the highly private PII/PHI of current and former patients, including information protected by HIPAA, unencrypted in its computer systems. Given the length of time it has been in business, it has accumulated approximately 138 years of patient and employee data.

31. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to state and federal law. It did not.

32. On or around July 13, 2024, Auxilio Mutuo Hospital issued a vague press release stating it discovered unauthorized access on its network on or around September 24, 2023.[6] It claimed "Although our investigation remains ongoing, we have concluded that a limited amount of personal information may have been removed from our network in connection with the incident, including full names and one or more of the following: medical records, diagnostic information, and other data related to patient care."[7] On information and belief, Auxilio Mutuo Hospital did not send written notification to potentially impacted individuals at this time, but instead encouraged "everyone to employe best security practices to protect personal information, including monitoring credit reports and financial statements."[8]

33. Auxilio Mutuo Hospital issued a second press release on April 21, 2025, explaining that the Department of Homeland Security notified it on September 23, 2023, that its systems could

[6] Hospital Español Auxilio Mutuo de Puerto Rico, Inc. Reports Network Breach (July 13, 2024), EUROPEAN BUSINESS MAGAZINE, https://europeanbusinessmagazine.com/accessnewswire/hospital-espanol-auxilio-mutuo-de-puerto-rico-inc-reports-network-breach/ (last visited April 30, 2025).
[7] *Id.*
[8] *Id.*

be the target of a cyberattack.[9] On November 21, 2023, Auxilio Mutuo Hospital's initial investigation revealed evidence consistent with unauthorized network access, although at that time, it claimed it could not determine if there had been any unauthorized data access or theft of information from its network.[10] *See also* Exs. A & B.

34. Auxilio Mutuo Hospital conducted a second investigation, and on May 15, 2024, where it identified evidence of unauthorized activity consistent with data exfiltration from systems that contained patient data, meaning it confirmed patient data was stolen.[11] On September 24, 2024, it claimed the breach was limited to patients who visited the hospital between August 2022 and September 2023.[12] *See also* Ex. A & B.

35. Despite the length of its two investigations, and despite its reliance on expert help, Auxilio Mutuo Hospital still remarkably maintains it is unable to determine the scope of the Data Breach, but admits that the stolen data potentially includes names in addition to some or all of the following:

- Contact information (first and last name, address, date of birth, phone number, and email address)
- Health information (medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment information)
- Health insurance information (primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers)

---

[9] Notice of Data Breach (April 21, 2025), ACCESS NEWSWIRE, https://www.accessnewswire.com/newsroom/en/education/notice-of-data-breach-1017895 (last visited April 30, 2025).
[10] *Id.*
[11] *Id.*
[12] *Id.*

- Billing, claims, and payment information (claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due)
- Other personal information (Social Security numbers, driver's licenses or state ID numbers, or passport numbers).[13] *See also* Exs. A & B.

36. As evidenced by the Data Breach, Defendant's cybersecurity systems were completely inadequate and allowed cybercriminals to steal files containing a treasure trove of highly private information belonging to its patients.

37. To make matters worse, Defendant waited until April 21, 2025, or at least 575 days, before it started notifying victims of the Data Breach.

38. Thus, Defendant kept the Class in the dark for over a year—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

39. Despite its duties to safeguard PII/PHI, Defendant did not in fact follow industry standard practices in securing the PII/PHI of its current and former patients, as evidenced by the Data Breach, its failure to discover the Data Breach, its failure to determine the scope of the Data Breach, and its extreme delay in notifying victims.

40. In response to the Data Breach, Defendant vaguely contends that it has "taken steps to strengthen our network systems to reduce the risk of a similar incident occurring in the future." Exs. A & B. Although Defendant does not explain what "steps" it has taken, such measures, if implemented at all, should have been in place before the Data Breach.

41. Through its Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, providing monitoring services, and advising Plaintiff "to remain

[13] *Id.*

vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. Exs. A & B.

42. Despite recognizing the harm that flowed from the Data Breach, Defendant waited an unreasonable amount of time before it began notifying victims, depriving Plaintiff and the Class of the earliest opportunity to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

43. On information and belief, Defendant has offered identity monitoring services to some victims, for twelve months, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the information compromised involves PII/PHI that cannot be changed, such as Social Security numbers. Exs. A & B.

44. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII/PHI is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

45. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII/PHI (although here, Social Security numbers were compromised). Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff and the Class's financial accounts.

46. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over the PII/PHI of its employees, clients, and patients. Defendant's negligence is evidenced by its failure to prevent the Data Breach, failure to detect the

Data Breach for an unknown period of time, and its inability to determine the exact information that was accessed, and the number of impacted individuals, for an unreasonable amount of time

47. Furthermore, Defendant obfuscates the nature of the Data Breach and the threat it posed. Exs. A & B. The Breach Notice fails to disclose how many people were impacted, how the Data Breach happened, how long the Data Breach lasted, how cybercriminals were able to avoid detection for an unknown period of time, how the Department of Homeland Security was able to discover the Data Breach but Auxilio Mutuo Hospital was not, and why it took Auxilio Mutuo Hospital more than 18 months before it finally began notifying some victims that cybercriminals had gained access to their highly private information.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

48. It is well known that PII/PHI is an invaluable commodity and a frequent target of hackers.

49. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

50. In fact, out of twenty industries that were analyzed, the healthcare industry is number eleven for highest count of ransomware attacks from January 2022 to January 2023.[14]

51. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[15]

52. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to

[14] *Ransomware Statistics: Who is targeted the most?* NORDLOCKER, https://nordlocker.com/ransomware-attack-statistics/ (last visited March 24, 2025).
[15] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited March 24, 2025).

prepare for and are able to thwart such an attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[16]

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

54. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII/PHI private and secure, Defendant failed to take appropriate steps to protect the PII/PHI of Plaintiff and Class Members from being compromised.

55. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included extortion and threatening to release stolen data.

56. In light of the information readily available and accessible before the Data Breach, Defendant, knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII/PHI could be accessed, exfiltrated, and published as the result of a cyberattack. Data breaches are so prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

Plaintiff's Experiences and Injuries

57. Plaintiff is a former patient of Auxilio Mutuo Hospital and is a Data Breach victim.

---

[16] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (published Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 24, 2025).

58. According to the Breach Notice he received on or around April 21, 2025, his first and last name, in combination with the following data elements, may have been impacted in the Data Breach:

- Health information (medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment information);
- Health insurance information (primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Billing, claims, and payment information (claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and
- Other personal information (Social Security numbers, driver's licenses or state ID numbers, or passport numbers).

59. As a condition of receiving services, Defendant required Plaintiff to provide his PII/PHI, including at least his name, date of birth, Social Security Number, and health information.

60. Plaintiff provided his PII/PHI to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

61. Additionally, Plaintiff reasonably expected that his personal information would be destroyed once his treatment from Defendant ended.

62. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff's PII/PHI for theft by cybercriminals and given the purpose of the hack, for sale on the Dark Web.

63. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him about the Data Breach.

64. Plaintiff suffered actual injury from the exposure of his PII/PHI —which violates his rights to privacy.

65. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

66. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring his credit information.

67. Plaintiff will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII/PHI was exposed. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

68. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII/PHI being placed in the hands of unauthorized third parties. This injury is worsened by Defendant's failure to promptly inform Plaintiff about the Data Breach.

69. Once an individual's PII/PHI is for sale and access on the Dark Web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[17] Plaintiff's PII/PHI was compromised as a result of the Data Breach.

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

71. Plaintiff also has a continuing interest in lifetime credit monitoring and identity theft monitoring on account of the Data Breach.

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

72. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII/PHI that can be directly traced to Defendant.

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

a. The loss of the opportunity to control how their PII/PHI is used;

b. The diminution in value of their PII/PHI;

c. The compromise and continuing publication of their PII/PHI;

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

---

[17] *What do Hackers do with Stolen Information,* AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited March 44, 2025).

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII/PHI; and

h. The continued risk to their PII/PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII/PHI in its possession.

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

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

76. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

77. It can take victims years to spot identity or PII/PHI theft, giving criminals plenty of time to use that information for cash.

78. One such example of criminals using PII/PHI for profit is the development of "Fullz" packages.

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

80. The development of "Fullz" packages means that stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's 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 stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

81. Defendant disclosed the PII/PHI of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, extortion, and exposure of stolen PII/PHI.

82. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest opportunity to take

appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

83. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[18] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[19]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[20]

c. 89% of consumers stated that "I care about data privacy."[21]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[22]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[23]

---

[18] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).
[19] *Id*. at 3.
[20] *Id*.
[21] *Id*. at 9.
[22] *Id*.
[23] *Id*.

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[24]

Defendant Failed to Follow FTC Guidelines

84. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII/PHI.

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

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

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

---

[24] *Id*. at 11.

88. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

89. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

90. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees regarding cybersecurity; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

91. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

92. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-

4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

93. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

94. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[25]

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

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

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

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

---

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

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

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

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

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

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

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

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

CLASS ACTION ALLEGATIONS

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

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach of Auxilio Mutuo Hospital's network, including all those individuals who received notice of the breach.

98. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including its staff and immediate family.

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

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

101. This action satisfies the numerosity, commonality, typicality, and adequacy requirements.

102. **Numerosity.** The Class members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 8,496 members.

103. **Commonality and Predominance.** Plaintiff's and the Class Members' claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

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

c. if Defendant was negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

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

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

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

105. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

106. **Appropriateness.** The likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

107. **Ascertainability.** All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some victims and sent them data breach notices.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

108. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

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

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

111. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

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

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

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

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

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII/PHI.

114. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and

necessary for Plaintiff and Class Members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

115. Defendant also had a duty to exercise appropriate clearinghouse practices and to remove PII/PHI it was no longer required to retain under applicable regulations.

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

117. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII/PHI, a necessary part of receiving services from Defendant.

118. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

119. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff's and Class Members' and the importance of exercising reasonable care in handling it.

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

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

122. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff 'and Class Members' PII/PHI by:

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

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

123. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII/PHI of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injury.

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

125. Defendant has admitted that the PII/PHI of Plaintiff and the Class was accessed by an intruder to its systems.

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

127. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost value of their PII/PHI, and lost time and money

incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

128. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

129. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII/PHI.

130. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII/PHI.

131. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

132. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

133. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

134. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

135. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

136. Defendant's violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

137. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

138. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

139. Defendant offered to provide services to Plaintiff and members of the Class if, and in exchange, Plaintiff and members of the Class provided Defendant with their PII/PHI.

140. In turn, Defendant agreed it would not disclose the PII/PHI it collects to unauthorized persons.

141. Plaintiff and the members of the Class accepted Defendant's offer by providing PII/PHI to Defendant in exchange for Defendant's services.

142. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

143. Plaintiff and the members of the Class would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

144. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly

of the intrusions into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII/PHI;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII/PHI that Defendant created, received, maintained, and transmitted.

145. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

146. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

147. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

148. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

149. Defendant obfuscated the nature of the Data Breach and failed to send Notice to the victims promptly and sufficiently.

150. In these and other ways, Defendant violated its duty of good faith and fair dealing.

151. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

152. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

153. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

154. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

155. Upon information and belief, Defendant funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

156. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

157. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased services from Defendant and/or its agents and in so doing provided Defendant or its agents with their PII/PHI. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII/PHI protected with adequate data security.

158. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII/PHI of Plaintiff and Class Members for business purposes.

159. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering services, a portion of which was to have been used for

data security measures to secure Plaintiff's and Class Members' PII/PHI, and by providing Defendant with their valuable PII/PHI.

160. Defendant was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII/PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid the data security obligations at the expense of Plaintiff and the Class by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

161. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

162. Defendant acquired the monetary benefit and PII/PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

163. If Plaintiff and Class Members knew that Defendant had not secured their PII/PHI, they would not have agreed to provide their PII/PHI to Defendant either directly or through their own financial institutions.

164. Plaintiff and Class Members have no adequate remedy at law.

165. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII/PHI is used; (ii) the compromise, publication, and/or theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII/PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long

as Defendant fails to undertake appropriate and adequate measures to protect PII/PHI in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

166. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

167. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

168. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

169. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

170. Specifically, Plaintiff and Class Members had a reasonable expectation of privacy given Defendant's representations and Privacy Policy. Defendant's disclosure of Plaintiff's PII is highly offensive to the reasonable person.

171. Defendant owed a duty to Plaintiff and Class Member to keep their PII/PHI confidential.

172. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII/PHI, is highly offensive to a reasonable person. It constitute an invasion of privacy both by disclosure of nonpublic facts, and intrusion upon seclusion.

173. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII/PHI constitutes an intentional interference with Plaintiff's and the Class Members' interest in

solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

174. Defendant's failure to protect Plaintiff's and Class Members' PII/PHI acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

175. Defendant knowingly did not notify Plaintiff's and Class Members in a timely fashion about the Data Breach.

176. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII/PHI, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

177. As a proximate result of Defendant's acts and omissions, the PII/PHI of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

178. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI is still maintained by Defendant with their inadequate cybersecurity system and policies.

179. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their PII/PHI. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the Class.

180. Plaintiff and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII/PHI.

181. Plaintiff and Class Members seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

182. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

183. Given the relationship between Defendant and Plaintiff and the Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely notify Plaintiff and Class Members of the Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

184. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

185. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

186. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

187. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach within a reasonable and practicable time period.

188. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

189. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

190. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

191. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

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

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. That to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures;

d. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

e. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

193. The Court should also issue corresponding injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual

audits of those systems and monitoring procedures; (iii) immediately provide adequate life-time credit monitoring to all Class Members; and (iv) barring Defendant from disclosing the PII/PHI of Plaintiff and the Class without their consent.

194. If an injunction is not issued, Plaintiff and the Class Members will be protected from a second breach. Additionally, Plaintiff and the Class will suffer irreparable injury, as their stolen information is more likely to be misused for identity theft or fraud without lifetime credit monitoring.

195. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

196. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

197. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

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

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

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

D. Enjoining Defendant from further unfair and/or deceptive practices;

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

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

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

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

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

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: May 1, 2025

By: */s/ **Carlos E. Matos***

Carlos E. Matos, Esq.
USDC-PR No.: 309902
Union Plaza Building, Suite 1202
416 Ponce de León Avenue
San Juan PR 00918

PO Box 11249
San Juan PR 00922-1249
(787) 378-1002
cemm787@gmail.com
LcdoMatos@pm.me

*/s/ **Raina C. Borrelli***
Raina C. Borrelli
Samuel J. Strauss*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com
sam@straussborrelli.com

**Pro Hac Vice forthcoming*
Attorneys for Plaintiff and the Proposed Class

Auxilio Mutuo
El Gran Hospital de Puerto Rico

Auxilio Mutuo
El Gran Hospital de Puerto Rico

NOTIFICACIÓN SOBRE POTENCIAL BRECHA DE DATOS

Hospital Español Auxilio Mutuo de Puerto Rico, Inc. publica este aviso para informarle que nuestra organización experimentó un incidente de seguridad.

Hospital Español Auxilio Mutuo de Puerto Rico, Inc. publica este aviso para informarle que nuestra organización experimentó un incidente de seguridad de datos en el cual su información pudo haber estado incluida como se describe más adelante. Nos tomamos muy en serio la privacidad y la seguridad, por lo que le proporcionamos un aviso sobre el incidente, las medidas que puede tomar para ayudar a proteger su información y la oportunidad de inscribirse en servicios gratuitos de monitoreo de crédito.

Qué ocurrió: El 23 de septiembre de 2023, el Departamento de Seguridad Nacional informó al Hospital Español Auxilio Mutuo de Puerto Rico, Inc. que nuestros sistemas pudieran ser el objetivo de un ataque cibernético. Inmediatamente después de recibir este aviso, iniciamos nuestro plan de respuesta a incidentes, contratamos asesores legales y contratamos a expertos en tecnología de la información externos (a través de los asesores legales) especializados en la respuesta a incidentes cibernéticos. El 21 de noviembre de 2023, nuestra investigación inicial identificó evidencia coherente con el acceso no autorizado a ciertos sistemas, pero no pudo concluir el alcance, de haberlo, del uso indebido o la exfiltración de datos.

En un intento por determinar aún más el alcance del incidente, lanzamos una segunda investigación, y el 15 de mayo de 2024, nuestros hallazgos preliminares identificaron actividad no autorizada en nuestros sistemas. Aunque finalmente no fue concluyente, el 24 de septiembre de 2024 se realizó una revisión integral de la evidencia disponible por parte de expertos internos y externos en IT lo cual limitó a los pacientes potencialmente afectados a aquellos que visitaron nuestras instalaciones entre agosto de 2022 y septiembre de 2023.

Aunque reiteramos que no hay evidencia en este momento para concluir afirmativamente que su información personal y médica haya sido exfiltrada en este incidente, por precaución, le proporcionamos este aviso y las medidas que puede tomar para proteger su información personal.

Qué información se vio involucrada: La información potencialmente afectada incluye su nombre y apellido, combinados con los siguientes elementos de datos:

- Información de seguros médicos (como planes/pólizas de salud primarios, secundarios u otros, compañías de seguros, números de identificación de miembros/grupos y números de identificación de pagadores del gobierno-Medicaid-Medicare).
- Información médica (como números de registros médicos, proveedores, diagnósticos, medicamentos, resultados de pruebas, imágenes, atención y tratamiento).
- Información de facturación, reclamaciones y pago (como números de reclamaciones, números de cuentas, códigos de facturación, tarjetas de pago, información financiera y bancaria, pagos realizados y saldo adeudado).

Y/O

- Otra información personal, como números de Seguro Social, números de licencia de conducir o de identificación

estatal, o números de pasaporte.

Qué estamos haciendo: Al enterarnos del incidente, tomamos medidas inmediatas para asegurar nuestros sistemas. También contratamos a asesores legales y contratamos especialistas forenses externos para ayudar a determinar la naturaleza y el alcance del incidente. Hemos tomado medidas para fortalecer nuestros sistemas de red para reducir el riesgo de que ocurra un incidente similar en el futuro.

También le brindamos la oportunidad de inscribirse en los servicios de **Medical Shield Pro** y **Equifax WebDefend** sin costo alguno para usted. Estos servicios le proporcionan alertas durante 12 meses a partir de la fecha de inscripción. Estos servicios serán proporcionados por CyEx y Equifax respectivamente; ambas compañías son especializadas en servicios de asistencia y remediación de fraudes. Las instrucciones sobre cómo inscribirse en estos servicios, junto con los recursos adicionales disponibles para usted, se incluyen en el documento adjunto "*Medidas que puede tomar para proteger su información*".

Qué puede hacer usted: Hasta la fecha, no tenemos conocimiento de ninguna denuncia de fraude de identidad o uso indebido de su información personal o médica como resultado directo de este incidente. Tampoco tenemos ninguna indicación de que su información personal o médica haya estado o esté en riesgo de ser utilizada indebidamente. Sin embargo, le recomendamos que permanezca alerta revisando sus estados de cuenta e informes de crédito para poder detectar actividad sospechosa y errores. Si descubre alguna actividad sospechosa o inusual en sus cuentas, comuníquese de inmediato con la institución financiera o compañía. A continuación proporcionamos información adicional sobre las medidas que puede tomar para protegerse contra el fraude y el robo de identidad, así como las instrucciones para registrarse en el monitoreo de crédito.

Para obtener más información: Si tiene preguntas o inquietudes, comuníquese con nuestra línea de asistencia exclusiva al 1-877-721-5315 entre las 9:00 a. m. y las 9:00 p. m., hora estándar del este, de lunes a viernes para obtener asistencia. Tenga en cuenta que la seguridad de la información es de suma importancia para nosotros. Mantenemos nuestro compromiso de conservar su confianza en nosotros y le agradecemos su apoyo durante este tiempo.

Atentamente,
Jorge J. Vélez Gutiérrez
Abogado General
Hospital Español Auxilio Mutuo de Puerto Rico, Inc

MEDIDAS QUE PUEDE TOMAR PARA PROTEGER SU INFORMACIÓN

Instrucciones de inscripción

Medical Shield Pro

Si necesita ayuda con el proceso de inscripción o tiene preguntas sobre Medical Shield, llame directamente a Medical Shield al 866.622.9303.

WebDefend de Equifax

Características clave

- El escaneo de Internet de Equifax WebDetect le alerta si su información se encuentra en sitios web utilizados por estafadores.
- Equifax Social Scan busca en los sitios de las redes sociales e informa sobre riesgos de fraude de información que usted podría estar compartiendo.

Si actualmente tiene o ha tenido en el pasado algún servicio de Equifax, no podrá registrarse en línea.

Comuníquese con el equipo de Atención al Cliente de Equifax de lunes a viernes, de 9:00 a. m. a 5:00 p. m. (GMT), al +44 (0)800 587 1584 o al +442037885496 si llama desde fuera del Reino Unido.

Monitoree sus cuentas y sus informes crediticios

Le recomendamos que esté atento para detectar incidentes de robo de identidad y fraude al revisar sus estados de cuenta y e informes de crédito, así como los formularios de explicación de beneficios para detectar actividad sospechosa y errores. En virtud de la ley estadounidense, tiene derecho a un informe crediticio gratuito anual de cada una de las tres oficinas de informes crediticios más importantes: TransUnion, Experian y Equifax. Para solicitar su informe crediticio sin cargo, visite www.annualcreditreport.com o llame al número gratuito 1-877-322-8228. Una vez revise su informe crediticio verifique discrepancias y trate de identificar aquellas cuentas que no abrió o consultas a entidades crediticias que no autorizó. Si tiene preguntas u observa información incorrecta, comuníquese con la oficina de informes crediticios.

Tiene derecho a colocar una “alerta de fraude” inicial o extendida en un expediente sin costo alguno. Una alerta de fraude inicial es una alerta de un (1) año que se coloca en el expediente crediticio de un consumidor. Al ver una alerta de fraude, es necesario que la empresa tome medidas para verificar la identidad del consumidor antes de conceder un nuevo crédito. Si es víctima de robo de identidad, tiene derecho a una alerta de fraude extendida que dura siete años. Si desea aplicar una alerta de fraude, comuníquese con cualquiera de las tres oficinas de informes crediticios indicadas a continuación:

Como alternativa a una alerta de fraude, usted tiene derecho a colocar un “congelamiento de crédito” en un informe de crédito, que prohibirá que una oficina de informes de crédito divulgue información en el informe de crédito sin su autorización expresa. El congelamiento de crédito está diseñado para evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. No obstante, debe tener en cuenta que el uso del congelamiento de crédito puede retrasar, interferir o vedar la aprobación oportuna de una solicitud o pedido posterior que usted haga con respecto a un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta relacionada con la concesión de un crédito. De conformidad con la legislación federal, no se le puede cobrar por aplicar o retirar un congelamiento de crédito en su informe crediticio. Para solicitar un congelamiento de crédito debe proporcionar la siguiente información:

1. Nombre completo (incluida la inicial de su segundo nombre, así como Jr., Sr., III, etc.).
2. Número de Seguro Social.
3. Fecha de nacimiento.

4. Dirección durante los dos a cinco años anteriores.
5. Constancia del domicilio actual, como por ejemplo, una factura de servicios públicos o de teléfono actuales. 6. Una fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir estatal o tarjeta de identificación, etc.).

7. Una copia de la denuncia a la policía, el informe de la investigación o la denuncia ante un organismo de ley por el robo de identidad, si es víctima de tal delito.

Si desea aplicar una alerta de fraude o congelamiento de crédito, comuníquese con las tres oficinas de informes crediticios indicadas a continuación:

TransUnion
1-800-680-7289
www.transunion.com

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094

Experian
1-888-397-3742
www.experian.com

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013

Experian Credit Freeze
P.O. Box 9554
Allen, TX 75013

Equifax
1-888-298-0045
www.equifax.com

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Información adicional

Para obtener más información acerca del robo de identidad, las alertas de fraude, el congelamiento de crédito y las medidas que puede tomar para proteger su información personal, comuníquese con las oficinas de informes crediticios, la Comisión Federal de Comercio (Federal Trade Commission, FTC) o con el fiscal general de su estado. La FTC también recomienda a aquellas personas que descubren que su información ha sido utilizada indebidamente que presenten un reclamo ante dicho organismo. Puede contactar a la FTC en 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338) y TTY: 1-866-653-4261. Tiene derecho a presentar una denuncia a la policía si alguna vez es víctima de fraude o robo de identidad. Recuerde que, para presentar una denuncia a la policía por robo de identidad, probablemente deberá proporcionar algún tipo de prueba que demuestre que ha sido víctima de tal delito. Las instancias de sospecha o certeza de robo de identidad también deben denunciarse a la policía, ante el fiscal general de su estado y a la FTC. Esta notificación no fue retrasada por la policía.

Para los residentes del Distrito de Columbia, pueden comunicarse con el Fiscal General del Distrito de Columbia en 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400 y https://oag.dc.gov/consumer-protection.

Para los residentes de Maryland, pueden comunicarse con el Fiscal General de Maryland en Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; o www.marylandattorneygeneral.gov.

Para residentes de Nuevo México, usted tiene ciertos derechos de acuerdo con la Ley de Información Crediticia Justa, como por ejemplo el derecho de obtener información si su expediente crediticio ha sido utilizado en su contra, el derecho de saber lo que contiene su expediente crediticio, el derecho de solicitar su calificación crediticia y el derecho de impugnar información incompleta o incorrecta. Además, en virtud de la Ley de Información Crediticia Justa: (i) las agencias de informes del consumidor deben corregir o eliminar toda información incorrecta, incompleta o no verificable; (ii) las agencias de informes del consumidor no pueden reportar información negativa desactualizada; (iii) el acceso a su expediente es limitado; (iv) usted

debe otorgar consentimiento para proporcionar informes crediticios a sus empleadores; (v) usted puede limitar las ofertas de crédito y seguro "preautorizadas" que usted reciba con base en información en su informe crediticio; y (vi) usted puede reclamar daños y perjuicios de quienes violen sus derechos. Es posible que también tenga otros derechos en virtud de la Ley de Información Crediticia Justa, que no son mencionados en el presente documento. Las víctimas de robo de identidad y el personal militar en servicio activo cuentan con otros derechos específicos en virtud de la Ley de Información Crediticia Justa. Le recomendamos revisar sus derechos en virtud de la Ley de Información Crediticia Justa ingresando en https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o por correo postal dirigido a Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Para los residentes de Nueva York, pueden comunicarse con el Fiscal General de Nueva York en Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; o en https://ag.ny.gov.

Para los residentes de Carolina del Norte, pueden comunicarse con el Fiscal General de Carolina del Norte en 9001 Mail Service Center, Raleigh, NC 27699-9001; llamando al 1-877-566-7226 o 1-919-716-6000; y en www.ncdoj.gov.

Para los residentes de Oregón, pueden comunicarse con el fiscal general de Oregón en Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; y https://doj.state.or.us/consumer-protection/.

Para los residentes de Rhode Island, pueden comunicarse con el Fiscal General de Rhode Island en 150 South Main Street, Providence, RI 02903; por teléfono al 1-401-274-4400; y en www.riag.ri.gov. En virtud de la ley de Rhode Island, usted tiene derecho a obtener la denuncia policial presentada con respecto a este incidente.

Hospital Español Auxilio Mutuo de Puerto Rico, Inc. is posting this substitute notice to provide customers and individuals with information about the data security incident experienced by our organization that may have involved their information as described below. We take privacy and security very seriously and are providing notice about the incident, steps you can take to help protect your information, and the opportunity to enroll in complimentary credit monitoring services.

What Happened: On September 23, 2023, the Department of Homeland Security informed Hospital Español Auxilio Mutuo de Puerto Rico, Inc. that our systems could be the target of a cyberattack. Immediately upon receiving this notice, we initiated our incident response plan, retained legal counsel, and engaged outside IT experts (through counsel) in cyber incident response. On November 21, 2023, our initial investigation identified evidence consistent with unauthorized access to certain systems, but was unable to conclude the extent, if any, of data misuse or exfiltration.

In an attempt to further determine the extent of the incident, we launched a second investigation, and on May 15, 2024, our preliminary findings identified unauthorized activity on Auxilio Mutuo's systems. Although ultimately inconclusive, on September 24, 2024, a comprehensive review of available evidence by internal and external IT experts limited the potentially affected patients to those who visited our facility between August 2022 and September 2023.

Although there is no evidence at this time to affirmatively conclude that personal and health information has been exfiltrated by this incident, out of an abundance of caution, we are providing this notice and steps you can take to protect personal information.

What Information Was Involved: The information potentially impacted includes your first and last name, in combination with the following data element(s):

- Health insurance information (such as primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Health information (such as medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment);
- Billing, claims and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and/or Other personal information such as Social Security numbers, driver's license or state ID numbers, or passport numbers.

What We Are Doing: Upon learning of the incident, we took immediate steps to address it, including securing our systems. We also retained legal counsel and engaged outside forensic specialists to assist with determining the nature and scope of the incident as outlined above. We have taken steps to strengthen our network systems to reduce the risk of a similar incident occurring in the future. We also are providing you with an opportunity to enroll in **Medical Shield Pro** and **Equifax WebDefend s**ervices at no cost to you. These services provide you with alerts for 12 months from the date of enrollment. These services will be provided by CyEx and Equifax respectively, both companies specialize in fraud assistance and remediation services. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed "*Steps You Can Take to Help Protect Your Information*."

What You Can Do: To date, we are not aware of any reports of identity fraud or improper use of your personal or health information as a result of this incident. Nor do we have any indication that your personal or health information has been or is threatened to be misused. However, it is always prudent for persons to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, as well as credit monitoring enrollment instructions.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line at 1- 877-721-5315 between the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time, Monday through Friday for assistance. Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,
Jorge J. Velez Gutierrez
General Counsel
Hospital Español Auxilio Mutuo de Puerto Rico, Inc

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enrollment Instructions

Medical Shield Pro

If you need assistance with the enrollment process or have questions regarding Medical Shield, please call Medical Shield directly at 866.622.9303.

Equifax WebDefend

Key Features

- Equifax WebDetect internet scanning alerts you if your information is found on websites used by fraudsters
- Equifax Social Scan searches social media sites and reports on fraud risks of information you may be sharing

Enrollment Instructions

If you currently have, or have previously had an Equifax service, you will not be able to register online.
Please contact Equifax Customer Care team Monday – Friday 9am – 5pm GMT at +44 (0)800 587 1584 or outside of the UK at +442037885496.

Monitor Your Accounts and Credit Reports

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one- year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1-800-680-7289	1-888-397-3742	1-888-298-0045

www.transunion.com www.experian.com www.equifax.com

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016-2000

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094

Experian Credit Freeze
P.O. Box 9554
Allen, TX 75013

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement. *For D.C. residents*, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and

https://doj.state.or.us/consumer-protection/.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

13707

Auxilio Mutuo
Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Morales Rosario A, Jose
[redacted]

April 21, 2025

NOTICE OF DATA BREACH

Dear Morales Rosario A, Jose:

We are writing to inform you of a data security incident experienced by our organization that may have involved your information as described below. We take privacy and security very seriously and are providing notice about the incident, steps you can take to help protect your information, and the opportunity to enroll in complimentary credit monitoring services.

What Happened: On September 23, 2023, the Department of Homeland Security informed Hospital Español Auxilio Mutuo de Puerto Rico, Inc. that our systems could be the target of a cyberattack. Immediately upon receiving this notice, we initiated our incident response plan, retained legal counsel, and engaged outside IT experts (through counsel) in cyber incident response. On November 21, 2023, our initial investigation identified evidence consistent with unauthorized access to certain systems, but was unable to conclude the extent, if any, of data misuse or exfiltration.

In an attempt to further determine the extent of the incident, we launched a second investigation, and on May 15, 2024, our preliminary findings identified unauthorized activity on Auxilio Mutuo's systems. Although ultimately inconclusive, on September 24, 2024, a comprehensive review of available evidence by internal and external IT experts limited the potentially affected patients to those who visited our facility between August 2022 and September 2023.

Although there is no evidence at this time to affirmatively conclude that your personal and health information has been exfiltrated by this incident, out of an abundance of caution, we are providing you with this notice and steps you can take to protect your personal information.

What Information Was Involved: The information potentially impacted includes your first and last name, in combination with the following data element(s):

- Health insurance information (such as primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers);
- Health information (such as medical record numbers, providers, diagnoses, medicines, test results, images, care and treatment);
- Billing, claims and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due); and/or
- Other personal information such as Social Security numbers, driver's license or state ID numbers, or passport numbers.

What We Are Doing: Upon learning of the incident, we took immediate steps to address it, including securing our systems. We also retained legal counsel and engaged outside forensic specialists to assist with determining the nature and scope of the incident as outlined above. We have taken steps to strengthen our network systems to reduce the risk of a similar incident occurring in the future. We also are providing you with an opportunity to enroll in **Medical Shield Pro** and **Equifax WebDefend** services at no cost to you. These services provide you with alerts for 12 months from the date of enrollment. These services will be provided by CyEx and Equifax respectively, both companies specialize in fraud assistance and remediation services. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed "*Steps You Can Take to Help Protect Your Information*."

What You Can Do: To date, we are not aware of any reports of identity fraud or improper use of your personal or health information as a result of this incident. Nor do we have any indication that your personal or health information has been or is threatened to be misused. However, it is always prudent for persons to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, as well as credit monitoring enrollment instructions.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line at 1-877-721-5315 between the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time, Monday through Friday for assistance. Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Jorge J. Velez Gutierrez
General Counsel
Hospital Español Auxilio Mutuo de Puerto Rico, Inc

Enclosure: *Steps You Can Take to Help Protect Your Information*

JS 44 (Rev. 09/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

JOSE A. MORALES ROSARIO

(b) County of Residence of First Listed Plaintiff CAROLINA, PR
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Carlos E Matos, Esq., Union Plaza Building Suite 1202
San Juan PR 00918, (787) 378-1002

DEFENDANTS

HOSPITAL ESPAÑOL AUXILIO MUTUO DE PUERTO RICO, INC.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ❒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 835 Patent - Abbreviated New Drug Application
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit (15 USC 1681 or 1692)
- ❒ 485 Telephone Consumer Protection Act
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ❒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act, 28 U.S.C. § 1332(d)(2).

Brief description of cause:
DEFENDANT IMPROPERLY SAFEGUARDED PLAINTIFF'S & CLASS MEMBERS' PII/PHI.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
05/01/2025

SIGNATURE OF ATTORNEY OF RECORD
Carlos E. Matos

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

CATEGORY SHEET

You must accompany your complaint with this Category Sheet, and the Civil Cover Sheet (JS-44).

Attorney Name (Last, First, MI): Matos, Carlos E.

USDC-PR Bar Number: 309902

Email Address: cemm787@gmail.com

1. Title (caption) of the Case (provide only the names of the first party on each side):

   Plaintiff: JOSE A. MORALES ROSARIO

   Defendant: HOSPITAL ESPAÑOL AUXILIO MUTUO DE PUERTO RICO, INC.

2. Indicate the category to which this case belongs:

   - [x] Ordinary Civil Case
   - [ ] Social Security
   - [ ] Banking
   - [ ] Injunction

3. Indicate the title and number of related cases (if any).

   N/A

4. Has a prior action between the same parties and based on the same claim ever been filed before this Court?

   - [ ] Yes
   - [x] No

5. Is this case required to be heard and determined by a district court of three judges pursuant to 28 U.S.C. § 2284?

   - [ ] Yes
   - [x] No

6. Does this case question the constitutionality of a state statute? (See, Fed.R.Civ. P. 24)

   - [ ] Yes
   - [x] No

Date Submitted: May 1, 2025

rev. Dec. 2009

Print Form Reset Form

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Puerto Rico

JOSE A. MORALES ROSARIO, individually and on behalf of all other similarly situated

Plaintiff(s)

v.

HOSPITAL ESPAÑOL AUXILIO MUTUO DE PUERTO RICO, INC.

Defendant(s)

Civil Action No. 3:25-cv-01244

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* HOSPITAL ESPAÑOL AUXILIO MUTUO DE PUERTO RICO, INC.
Av. Ponce de León 1715
San Juan PR 00918

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Carlos E. Matos, Esq.
Edificio Union Plaza, Ste 1202
Av. Ponce de León 416
San Juan PR 00918

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Ada I. García Rivera, Esq., CPA
CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 3:25-cv-01244

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* HOSPITAL ESPAÑOL AUXILIO MUTUO DE PUERTO RICO, II
was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____ , a person of suitable age and discretion who resides there,
on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: