UNITED STATES DISTRICT COURT

DISTRICT OF PUERTO RICO

PABLO J. QUINTERO, and JOANNIE PRINCIPE, individually and on behalf of all others similarly situated, Plaintiffs, v. METRO SANTURCE, INC., d/b/a PAVIA HOSPITAL SANTURCE a corporation, METRO HATO REY, INC., d/b/a PAVIA HOSPITAL HATO REY and DOES 1 to 10, inclusive, Defendants.	CASE NO.: 20-1075 **CLASS ACTION** **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Pablo J. Quintero and Joannie Principe ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action based upon their personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigation of their attorneys.

NATURE OF THE ACTION

1. Defendant Metro Santurce, Inc. ("Metro Santurce") owns and operates the Pavia Hospital Santurce. Defendant Metro Hato Rey, Inc. ("Metro Hato Rey") owns and operates the Pavia Hospital Hato Rey (Metro Santurce and Metro Hato Rey are herein referred to as "Defendants"). Thousands of patients count on Metro Santurce and Metro Hato Rey to treat them competently and to handle their sensitive medical and personal information with care.

2. These patients reasonably expect the highest level of protection for their private identifiable information, when giving highly sensitive information such as their Social Security numbers and medical information to medical providers and insurers. What these patients do not expect, and did not expect, was that their personal and sensitive information would be harvested by unauthorized individuals.

3. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter, "Class Members"), bring this class action to secure redress against Defendants for

their reckless and negligent violation of patient privacy rights. Plaintiffs and Class Members are patients of Metro Santurce and Metro Hato Rey who were exposed by a data breach.

4. Plaintiffs and Class Members suffered significant injuries and damages. On information and belief, the security breach compromised the full names, addresses, dates of birth, gender, financial information, and social security numbers (referred to collectively as "PII")[1] of Plaintiffs and the Class Members.

5. As a result of Defendants' wrongful actions and inactions, unauthorized individuals gained access to and harvested Plaintiffs' and Class Members' PII. Plaintiffs have been forced to take remedial steps to protect themselves from future loss. Indeed, all Class Members are currently at a very high risk of identity theft and/or credit fraud, and prophylactic measures, such as the purchase of credit monitoring, are reasonable and necessary to prevent and mitigate future loss.

6. As a result of Defendants' wrongful actions and inactions, patient information was stolen. Many Metro Santurce and Metro Hato Rey patients have had their PII compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages.

7. Further, despite the fact that the breach was discovered on February 12, 2019, Defendants did not begin notifying their customers of the event until June 18, 2019, over four months later.

THE PARTIES

8. Plaintiff Pablo J. Quintero is a Puerto Rico citizen residing in Guaynabo, Puerto Rico. Plaintiff Quintero received medical care from Metro Santurce, pursuant to which Metro Santurce obtained Plaintiff Quintero's PII.

9. Plaintiff Joannie Principe is a Puerto Rico citizen residing in Carolina, Puerto Rico. Plaintiff Principe received medical care from Metro Hato Rey, pursuant to which Metro Hato Rey obtained Plaintiff Principe's PII.

10. Plaintiffs are informed and believe that, as a result of the data breaches that took

[1] The PII here referenced also constitutes PHI as defined by HIPAA.

place at Metro Santurce and Metro Hato Rey, Plaintiffs' PII was accessed by hackers. As a result, Plaintiffs have to purchase credit and personal identity monitoring services to alert them to potential misappropriation of their identity and to combat risk of further identity theft. At a minimum, therefore, Plaintiffs have suffered compensable damages because they will be forced to incur the cost of a monitoring service, which is a reasonable and necessary prophylactic step to prevent and mitigate future loss. Exposure of Plaintiffs' PII as a result of the data breach has placed them at imminent, immediate and continuing risk of further identity theft-related harm.

11. Defendant Metro Santurce is a corporation with its principal offices located in Guaynabo, Puerto Rico. Metro Santurce owns and operates the Pavia Hospital Santurce.

12. Defendant Metro Hato Rey is a corporation with its principal offices located in Guaynabo, Puerto Rico. Metro Hato Rey owns and operates the Pavia Hospital Hato Rey.

13. Plaintiffs are unaware of the true names, identities, and capacities of the defendants sued herein as DOES 1 to 10. Plaintiffs will seek leave to amend this complaint to allege the true names and capacities of DOES 1 to 10 if and when ascertained. Plaintiffs are informed and believe, and thereupon allege, that each of the defendants sued herein as a DOE is legally responsible in some manner for the events and happenings alleged herein and that each of the defendants sued herein as a DOE proximately caused injuries and damages to Plaintiffs and Class Members as set forth below.

14. As used herein, "Defendants" shall refer to Metro Santurce, Metro Hato Rey, and DOES 1 to 10, collectively.

JURISDICTION AND VENUE

15. 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.

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

17. Venue is appropriate in this District because, among other things: (a) Plaintiffs resides in this District, (b) Defendants maintain offices in this District, where they conduct substantial business; (c) Defendants directed their 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.

18. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because Defendants conduct a large amount of their business in this District, and because Defendants have substantial relationships in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

19. On February 12, 2019, the Pavia Hospital Santurce, owned and operated by Defendant Metro Santurce, and the Pavia Hospital Hato Rey, owned and operated by Defendant Metro Hato Rey, suffered a computer hack in which money was demanded in exchange for the release of the computer systems. During this hack, critical patient PII was exposed to the hackers.

20. On June 18, 2019, over four months later, Defendants began sending letters to the breach victims to inform them of the data breaches.

21. Defendants made repeated promises and representations to their patients, which formed a part of their contracts with those patients, that they would protect Plaintiffs' and the Class Members' PII from disclosure to third parties, including taking appropriate steps to safeguard their electronic databases. The Pavia Hospital Santurce's and Pavia Hospital Hato Rey's websites each contains a page titled "HIPAA Law," which states that each hospital "understands that the information on the patient's health is exclusively personal and we are committed to protecting the patient's privacy," and that "[a]ccording to the law we must . . . [m]ake sure to maintain the privacy of medical information that identifies you." (*See* Privacy Notices, translated on December 26, 2019, **Ex. A and B**). The Privacy Notices proceed to list the specific ways in which the hospitals are permitted to disclose PII, none of which were present in the current case, and state that no other disclosures will take place without written authorization.

22. Defendants promised that they would not disclose Plaintiffs' and the Class Members' PII to any unauthorized third parties. In fact, they allowed hackers to obtain it.

B. Defendants Had an Obligation to Protect Personal Information under Federal Law.

23. Defendants are entitles covered by HIPAA (*see* 54 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information").

24. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information." 45 C.F.R. § 164.502. HIPAA also requires that Defendants implement appropriate safeguards for this information. 45 C.F.R. § 164.530(c)(1). HIPAA additionally requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable—i.e. non-encrypted data—to unauthorized third parties. 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

25. Additionally, HIPAA requires that Defendants:

(a) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, *see* 45 C.F.R. § 164.312(a)(1);

(b) Implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. § 164.306(a)(1);

(c) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, *see* 45 C.F.R. § 164.306(a)(2);

(d) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, *see* 45 C.F.R. § 164.306(a)(3);

(e) Ensure compliance with the HIPAA security standard rules by its workforce, *see* 45 C.F.R. § 164.306(a)(4); and

(f) Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b).

26. Defendants are additionally prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has found that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015). [2]

27. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

28. 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.[3] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. [4]

29. Additionally, the FTC recommends that companies 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

---

[2] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 22, 2019).

[3] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 22, 2019).

[4] *Id*.

have implemented reasonable security measures. [5]

30. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. [6]

31. In this case, Defendants were fully aware of their obligation to use reasonable measures to protect the personal information of their patients, acknowledging as much in their own privacy policies. Defendants also knew they were targets for hackers. But despite understanding the consequences of inadequate data security, Defendants failed to comply with industry-standard data security requirements.

32. Defendants failure to employ reasonable and appropriate measures to protect against unauthorized access to members' information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

C. Applicable Standards of Care

33. In addition to their obligations under federal law, Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel

[5] Federal Trade Commission, *Start With Security A Guide for Business* (Jun. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec. 10, 2019).

[6] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Nov. 22, 2019).

responsible for them, adequately protected the PII of Plaintiffs and the Class Members.

34. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

35. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed PII within their computer systems on how to adequately protect PII.

36. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to implement processes that would detect a breach of their data security systems in a timely manner.

37. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to act upon data security warnings and alerts in a timely fashion.

38. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to purchase insurance or other health care services from Defendants' or to entrust PII with Defendants.

39. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to disclose in a timely and accurate manner when data breaches occurred.

40. Defendants owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants received the PII from other parties with the understanding that Plaintiffs and the Class Members expected their PII to be protected from disclosure. Defendants knew that a breach of the hospitals' data systems would cause Plaintiffs and the Class Members to incur damages.

D. Stolen Information Is Valuable to Hackers and Thieves

41. It is well known, and the subject of many media reports, that PII is highly coveted and a frequent target of hackers. According to a report by the HIPAA Journal, "healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published."[7] As reflected in the chart below, many of the largest healthcare breaches over the last decade have involved millions of patient or member records.

///

Largest Healthcare Data Breaches (2009-2018)

Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
3	Excellus Health Plan Inc.	2015	Health Plan	10,000,000	Hacking/IT Incident
4	Science Applications International Corporation	2011	Business Associate	4,900,000	Loss
5	University of California, Los Angeles Health	2015	Healthcare Provider	4,500,000	Hacking/IT Incident
6	Community Health Systems Professional Services Corporations	2014	Business Associate	4,500,000	Hacking/IT Incident
7	Advocate Medical Group	2013	Healthcare Provider	4,029,530	Theft
8	Medical Informatics Engineering	2015	Business Associate	3,900,000	Hacking/IT Incident
9	Banner Health	2016	Healthcare Provider	3,620,000	Hacking/IT Incident
10	Newkirk Products, Inc.	2016	Business Associate	3,466,120	Hacking/IT Incident

[7] Healthcare Data Breach Statistics, HIPAA JOURNAL, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Aug. 9, 2019).

42. Despite well-publicized litigation and frequent public announcements of data breaches, Defendants maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class Members.

43. Legitimate organizations and members of the criminal underground alike recognize the value of PII. Otherwise, they would not aggressively seek and pay for it. As previously seen in one of the world's largest data breaches, hackers compromised the card holder data of 40 million of Target's customers. *See* "Target: 40 million credit cards compromised," CNN Money, Dec. 19, 2013, *available* at http://money.cnn.com/2013/12/18/news/companies /target-credit-card/**.** DataCoup is, in contrast, just one example of a legitimate business that pays users for personal information. *See* http://money.com/money/3001361/datacoup-facebook-personal-data-privacy/.

44. PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps." *See* Krebs on Security April 16, 2016, Blog Post, *available at* https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/. PII can be used to clone a debit or credit card. *Id.*

45. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

46. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information,

including birthdates and Social Security numbers."[8]

E. The Data Breach Has Resulted and Will Result in Identity Theft and Identity Fraud

47. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiffs and Class Members.

48. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII secure is severe. According to Javelin Strategy and Research, "one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year." "Someone Became an Identity Theft Victim Every 2 Seconds Last Year," Fox Business, Feb. 5, 2014 *available* at http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-last-year.html.

49. In the case of a data breach, simply reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." *See* "Victims of Identity Theft," U.S. Department of Justice, Dec 2013, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf. In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

50. A person whose PII has been obtained and compromised may not know or experience the full extent of identity theft or fraud for years. It may take some time for the victim to become aware of the theft or fraud. In addition, a victim may not become aware of fraudulent charges when they are nominal, because typical fraud-prevention algorithms fail to capture such charges. Those charges may be repeated, over and over again, on a victim's account, without notice for years.

51. The damage from PII exposure is particularly acute in the medical context. A study by Experian found that the "average total cost" of medical identity theft is "about

[8] https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf

$20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage. *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 a.m.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/. Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all. *Id*.

52. The Personal Information exposed in the Data Breach is highly-coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web" – exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Medical data is particularly valuable because unlike financial information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendants, are intended targets of cyber-criminals.

53. The Personal Information also has substantial legitimate value to Defendants. As Defendants' privacy policies recognize, they use Plaintiffs' Personal Information for business purposes other than administering claims. Many companies that retain Personal Information like that exposed in the data breach attribute inherent monetary value to it—even listing it as an asset on their books or using it as collateral or consideration for other transactions. Personal Information, including de-identified medical information, is a valuable commodity in the data-

driven market place and is often sold and traded between companies—subject to legal and contractual restrictions.

54. And consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple and discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases, and viewed and used by different criminal actors.

55. Exposure of this information to the wrong people can have serious consequences. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[9] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

56. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and

[9] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Nov. 22, 2019).

> monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[10]

57. As a result of the data breach, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are also subject to a higher risk of phishing and pharming where hackers exploit information they already obtained in an effort to procure even more PII. Plaintiffs and Class Members are presently incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies. In addition, Plaintiffs and Class Members now run the risk of unauthorized individuals creating credit cards in their names, taking out loans in their names, and engaging in other fraudulent conduct using their identities.

F. Plaintiffs and Class Members Suffered Damages

58. The exposure of Plaintiffs' and Class Members' PII to unauthorized third-party hackers was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by their contracts with Plaintiffs and the Class Members, and federal law. The data breach was also a result of Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts and federal law

59. Plaintiffs' and Class Members' PII is private and sensitive in nature and was inadequately protected by Defendants. Defendants did not obtain Plaintiffs' and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

60. As a direct and proximate result of Defendants' wrongful actions and inaction

[10] FTC, *Combating Identity Theft A Strategic Plan* (April 2007), available at https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Nov. 22, 2019).

and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

61. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure, compromising, and theft of their PII;

b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of unauthorized third-party hackers and misused via the sale of Plaintiffs' and Class Members' information on the Internet black market;

c. The untimely and inadequate notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

e. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market.

CLASS ACTION ALLEGATIONS

62. Plaintiffs bring this action on their own behalf and on behalf of all others similarly situated under Rule 23(a), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure. The Class is divided into two Classes as follows:

> The Puerto Rico Class:
>
> All persons residing in the Territory of Puerto Rico whose Personal Identifying Information was compromised as a result of the data breach of the Pavia Hospital Santurce and the Pavia Hospital Hato Rey, discovered on February 12, 2019.

The National Class:

> All persons residing in the United States whose Personal Identifying Information was compromised as a result of the data breach of the Pavia Hospital Santurce and the Pavia Hospital Hato Rey, discovered on February 12, 2019.

63. Excluded from the Class are: (a) Defendants, including any entity in which any of the Defendants has a controlling interest, is a parent or a subsidiary of, or which is controlled by any of the Defendants; (b) the officers, directors, and legal representatives of Defendants; and (c) the judge and the court personnel in this case as well as any members of their immediate families. Plaintiffs reserves the right to amend the definition of the Class if discovery, further investigation and/or rulings by the Court dictate that it should be modified.

64. *Numerosity*. The members of the Class are so numerous that the joinder of all Class Members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, given the number of patients who trust their care to Defendants, it stands to reason that the number of Class Members is in the thousands. Class Members are readily identifiable from information and records in Defendants' possession, custody, or control, such as account information.

65. *Commonality and Predominance*. There are questions of law and fact common to Class Members, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants owed a duty of care to Plaintiffs and Class Members with respect to the security of their PII;

b. What security measures must be implemented by Defendants to comply with their duty of care;

c. Whether Defendants met the duty of care owed to Plaintiffs and the Class Members with respect to the security of the PII;

d. Whether Defendants have a contractual obligation to Plaintiffs and Class Members to use reasonable security measures;

e. Whether Defendants have complied with any contractual obligation to use reasonable security measures;

f. What security measures must be implemented by Defendants to comply with their contractual obligations to use reasonable security measures;

g. Whether Defendants' acts and omissions described herein violated the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

h. Whether Defendants' acts and omissions described herein violated the Federal Trade Commission Act, 15 U.S.C. § 45;

i. What security measures, if any, must be implemented by Defendants to comply with their contractual and statutory obligations;

j. The nature of the relief, including equitable relief, to which Plaintiffs and Class Members are entitled; and

k. Whether Plaintiffs and Class Members are entitled to damages, civil penalties and/or injunctive relief.

66. *Typicality*. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of each of the other Class Members, was exposed and/or improperly disclosed by Defendants.

67. *Adequacy of Representation*. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs have retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and Class Members have a unified and non-conflicting interest in pursuing the same claims and obtaining the same relief. Therefore, all Class Members will be fairly and adequately represented by Plaintiffs and their counsel.

68. *Superiority of Class Action*. A class action is superior to other available methods for the fair and efficient adjudication of the claims alleged in this action. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially

conflicting adjudications of the asserted claims. There will be no difficulty in the management of this action as a class action, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied.

69. Class certification is also appropriate because Defendants have acted or refused to act on grounds generally applicable to the Class Members, such that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

FIRST CAUSE OF ACTION

(Breach of Express And/or Implied Contractual Promise)

70. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 69, inclusive, of this Complaint as if set forth fully herein.

71. Defendants were parties to contracts with Plaintiffs and the Class Members for medical services, pursuant to which Defendants obtained Plaintiffs' and the Class Members' PII.

72. As a part of these contracts, Defendants promised to maintain adequate safeguards to protect the PII from disclosure to unauthorized third parties, and also promised not to disclose the PII to unauthorized third parties. Defendants promised that "the information on the patient's health is exclusively personal and we are committed to protecting the patient's privacy," and that "[a]ccording to the law we must . . . [m]ake sure to maintain the privacy of medical information that identifies you." They also promised that "[a]ny other use or disclosure" of PII "that is not described in this Notice of Privacy Practice requires the patient's written authorization." **Ex. A and B**.

73. Accordingly, Defendants' promises to safeguard and protect the PII are contractually binding upon Defendants with regard to Plaintiffs and each of the Class members.

74. The contractual duty to protect and safeguard Plaintiffs' and the Class Members' PII, which Defendants promised to undertake, was, even apart from the language of the

contracts, a term of the contracts by operation of law under the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E., and under the Federal Trade Commission Act, 15 U.S.C. § 45. Under applicable common law, all laws in place at the time a contract is entered which are relevant to the subject matter of that contract become binding terms of the contract. Therefore, the HIPAA Privacy Rule and Security Rule, and the FTCA also formed a contractual term in each of Defendants' contracts with Plaintiffs and the Class Members.

75. Finally, the promise to safeguard and protect Plaintiffs' and the Class Members' PII, and keep that PII from being accessed by third parties, was implied as a matter of law because Defendants and Plaintiffs and the Class Members entered their agreements with the expectation and implied mutual understanding that Defendants would strictly maintain the confidentiality of the PII and safeguard it from theft or misuse.

76. Therefore, Plaintiffs and Class Members entered contracts for medical services with Defendants in which Defendants agreed to: (a) implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' personal information from unauthorized access, destruction, use, modification, or disclosure; and (b) prevent unauthorized third parties from obtaining access to Plaintiffs' and Class Members' PII.

77. Plaintiffs and the Class Members would not have provided and entrusted the PII to Defendants in the absence of the proper security safeguards and the promise to keep their PII safe.

78. Plaintiffs and the Class Members fully performed their obligations under their agreements with Defendants.

79. Defendants breached the contractual promises by failing to: (a) implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure; and (b) prevent unauthorized third parties from obtaining access to Plaintiffs' and Class Members' PII.

80. Plaintiffs' and the Class Members' expectation was that their PII would be safeguarded and protected. Therefore, they agreed to pricing terms to which they would not

have agreed had they known that their PII would not be protected. Further, due to the fact that their PII was not protected, Plaintiffs and the Class Members incurred losses associated with the loss of PII privacy, including theft, identity theft, and the risk of theft and identity theft, along with the necessity of cancelling credit cards and paying for additional protection through the market. The risk of identity theft which Plaintiffs now faces is considerable. Hackers do not target PII without the intent to use it fraudulently.

81. As a direct and proximate result of Defendants' breaches of the contractual promises alleged herein, Plaintiffs and Class Members sustained actual losses and damages in an amount according to proof at trial but in excess of the minimum jurisdictional requirement of this Court.

SECOND CAUSE OF ACTION

(Breach of Covenant of Good Faith and Fair Dealing)

82. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 81, inclusive, of this Complaint as if set forth fully herein.

83. Applicable law implies a covenant of good faith and fair dealing in every contract.

84. Plaintiffs and Class Members entered contracts with Defendants for medical services.

85. Plaintiffs and the Class Members performed all of their duties under their agreements with Defendants.

86. All of the conditions required for Defendants' performance under the contracts have occurred.

87. Incorporated in the contracts as a matter of law was the covenant of good faith and fair dealing, which prevents a contracting party from engaging in conduct that frustrates the other party's rights to the benefits of the agreement. The implied covenant imposes on a contracting party not only the duty to refrain from acting in a manner that frustrates performance of the contract, but also the duty to do everything that the contract presupposes that the contracting party will do to accomplish its purposes.

88. Here the implied covenant of good faith and fair dealing required Defendants, under the terms of their agreement which stated that Defendants would protect the PII, to safeguard and protect from disclosure to third parties the PII of Plaintiffs and the Class Members which was turned over to Defendants only for the purposes of performing medical services. Plaintiffs and the Class Members could not enjoy Defendants' services without the safeguarding and protection of the PII.

89. Defendants breached the covenant of good faith and fair dealing implied in their contracts by engaging in the following conscious and deliberate acts: (a) failing to implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure; and (b) failing to ensure that unauthorized parties were not provided access to Plaintiffs' and Class Members' PII. Defendants' failure to protect the PII of Plaintiffs and Class Members frustrated Plaintiffs' and the Class Members' rights to the benefit of their bargains with Defendant, to enjoy the professional services of Defendant without incurring risks of property and identity theft.

90. Plaintiffs and Class Members have lost the benefit of their contracts by having their PII compromised and have been placed at an imminent, immediate and continuing risk of identity theft-related harm. The risk of identity theft which Plaintiffs now faces is considerable. Hackers do not target PII without the intent to use it fraudulently.

91. As a direct and proximate result of Defendants' breach of the covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

THIRD CAUSE OF ACTION

(Negligence)

92. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 91, inclusive, of this Complaint as if set forth fully herein.

93. As described above, Defendants owed Plaintiffs and the Class Members duties of care in the handling of PII, which duties included keeping that PII safe and preventing

disclosure of that PII to all unauthorized third parties.

94. Additionally, Defendants owed a duty to Plaintiffs and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII as required by HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E, and Federal Trade Commission Act, 15 U.S.C. § 45. This legal duty arises outside of any contractual, implied or express, responsibilities that Defendants had between Plaintiffs and Class Members, as it is completely independent of any contract.

95. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information." 45 C.F.R. § 164.502. HIPAA also requires that Defendants implement appropriate safeguards for this information. 45 C.F.R. § 164.530(c)(1). HIPAA additionally requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable—i.e. non-encrypted data—to unauthorized third parties. 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

96. Additionally, HIPAA requires that Defendants:

(a) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, *see* 45 C.F.R. § 164.312(a)(1);
(b) Implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. § 164.306(a)(1);
(c) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, *see* 45 C.F.R. § 164.306(a)(2);
(d) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, *see* 45 C.F.R. § 164.306(a)(3);
(e) Ensure compliance with the HIPAA security standard rules by its workforce, *see* 45 C.F.R. § 164.306(a)(4); and
(f) Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b).

97. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

98. Defendants violated the above listed regulations by disclosing the PII to third

parties and by failing to implement adequate security measures to protect the PII, including failing to:

(a) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;
(b) Implement policies and procedures to prevent, detect, contain, and correct security violations;
(c) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information;
(d) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information;
(e) Ensure compliance with the HIPAA security standard rules by its workforce; and
(f) Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information.

99. Defendants also violated §§ 164.404 and 164.402 by failing to provide timely notice of the breach to Plaintiffs and the Class Members.

100. The harm that occurred as a result of the security breach is the type of harm that HIPAA was intended to guard against. HIPAA directly requires subject entities to protect the health information of individuals such as Plaintiffs and the Class Members.

101. 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 Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

102. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

103. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a company as large as Defendants', including, specifically, the damages that would result to

Plaintiffs and Class members.

104. The harm that occurred as a result of the security breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

105. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

106. In addition to their obligations under state and federal law, Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and the Class Members.

107. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

108. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed PII within their computer systems on how to adequately protect PII.

109. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to implement processes that would detect a breach of their data security systems in a timely manner.

110. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted

them with sensitive PII, to act upon data security warnings and alerts in a timely fashion.

111. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to purchase insurance or other health care services from Defendants' or to entrust PII with Defendants.

112. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to disclose in a timely and accurate manner when data breaches occurred.

113. Defendants owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants collected Plaintiffs' and the Class Members' PII. Defendants knew that a breach of their data systems would cause Plaintiffs and the Class Members to incur damages.

114. Defendants breached those duties of care by adopting inadequate safeguards to protect the PII, and, on information and belief, failing to adopt industry-wide standards in their supposed protection of the PII, resulting in the disclosure of the PII to unauthorized third parties.

115. As a direct and proximate result of Defendants' failure to adequately protect and safeguard the PII, Plaintiffs and the Class members suffered damages. Plaintiffs and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft and theft of property, and for which Plaintiffs and the Class members were forced to adopt costly and time-consuming preventive and remediating efforts. Plaintiffs and the Class Members were also damaged in that they paid for services in an amount that they would have refused to pay had they known that Defendants would not protect their PII. Plaintiffs and the Class Members accepted pricing terms which they would not have agreed to had they known that Defendants would not protect their PII. The risk of identity theft which Plaintiffs now faces is considerable. Hackers do not target PII without the intent to use it fraudulently.

116. Defendants acted with wanton disregard for the security of Plaintiffs' and the Class Members' PII. Defendants knew or should have known that Defendants had inadequate computer systems and data security practices to safeguard such information, and Defendants knew or should have known that hackers were attempting to access the PII of health care providers' databases, such as Defendants'.

117. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and the Class Members to experience the foreseeable harm associated with the exposure of their PII.

118. A "special relationship" exists between Defendants and Plaintiffs and the Class Members. Defendants entered into a "special relationship" with Plaintiffs and the Class Members when they contracted with Plaintiffs' and the Class Members to provide them with medical care and obtained Plaintiffs' and the Class Members' PII from them. As providers of health care services, Defendants stand in a fiduciary or quasi-fiduciary relationship with Plaintiffs and the Class Members.

119. Plaintiffs and the Class Members have suffered monetary injury in fact as a direct and proximate result of the acts committed by Defendants as alleged herein in an amount to be proven at trial but in excess of the minimum jurisdictional amount of this Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, pray for relief as follows:

1. For compensatory damages in an amount according to proof at trial;

2. For affirmative injunctive relief mandating that Defendants implement and maintain reasonable security procedures and practices to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure;

3. For costs of suit and litigation expenses;

4. For attorneys' fees under the common fund doctrine and all other applicable law;

and

5. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a jury trial for all claims so triable.

Dated: February 11, 2020

Respectfully submitted,

/s/ *David C. Indiano*
David C. Indiano USDC Bar No. 200601
Jeffrey M. Williams USDC Bar No. 202414
Vanesa Vicéns-Sánchez USDC Bar No. 217807
Christopher A. Dávila USDC Bar No. 304103
INDIANO & WILLIAMS, P.S.C.
207 del Parque Street, Third Floor
San Juan, Puerto Rico 00912
Telephone: (787) 641-4545
Facsimile: (787) 641-4544

/s/ *Thiago M. Coelho*
Bobby Saadian*
Justin F. Marquez*
Thiago M. Coelho*
Robert J. Dart*
WILSHIRE LAW FIRM
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

(**pro hac vice applications forthcoming*)

Attorneys for Plaintiffs and the Proposed Class

HIPAA

Effective Date: April 14, 2003
Effective amendment date: April 14, 2003
Review date: September 23, 2013

THIS NOTICE DESCRIBES HOW THE PATIENT'S MEDICAL INFORMATION MAY BE USED AND DISCLOSED AND HOW THEY CAN GET ACCESS TO THIS INFORMATION. PLEASE READ THE CONTENT CAREFULLY.

The Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act (found in Title XIII of the American Recovery and Reinvestment Act of 2009) (collectively referred to as "HIPAA"), with the amendments that are implemented in a timely manner, require that Hospital Pavia Arecibo maintain the privacy of individually identifiable patient health information (this information is considered "protected health information" and is referred to herein as "PHI"). The HIPAA Privacy Rule requires that we provide a detailed written notice about our privacy practices.

Hospital Pavia Arecibo understands that the patient's health information is exclusively personal and we undertake to protect] the patient's privacy. Read this Notice of Privacy Practices carefully. This notice informs you of how we may use your medical information and/or disclose it to third parties. It also describes your rights and certain obligations we have regarding the use and disclosure of medical information.

According to the law, we must:

1. Be sure to maintain the privacy of medical information that identifies you.
2. Give you this notice about our legal duties and privacy practices regarding your medical information.
3. Comply with the terms of this notice that are currently in effect.

This Notice applies to the provision of health care by Hospital Pavia Arecibo, medical staff, outpatient departments and clinics. This Notice also applies to the utilization review and quality assessment activities of Hospital Pavia Arecibo.

I. Permitted Use or Disclosure

The following sections describe different ways that we are authorized to use and disclose your medical information. Not all categories are mentioned, however, all those in which we are allowed to use and/or disclose your information to others, are derived from one of the following categories:

A. **For Treatment:** We may use medical information about you to provide you with medical treatment. We may also exchange it with doctors, nurses, technicians, students, or other staff members, such as the departments of the Hospital may share your medical information to coordinate elements of your care, such as prescriptions, blood tests and x-rays. We may also exchange your medical information with people

outside **Hospital Pavia Arecibo**, such as with the doctors who referred you and with those who treat you.

B. **For Payment:** We may use your information and/or transfer it to your health insurance policy or to other people who help you pay for your care. For example, we may inform your health insurance about a treatment you are going to receive to determine if your health care insurance would pay for that treatment.

C. **For Health Care Operations:** We may use your medical information to improve the quality of care we provide. These activities help us carry out our programs to ensure that all our patients receive quality health care. For example, we may use your information to review our treatments and services. Also, to evaluate the effectiveness of our employees and their care for you. We may also disclose your health information to doctors, nurses, technicians, students, and other health care employees for educational purposes or as preparation for research.

D. **Other Uses and Disclosures:** As part of the treatment, payment and medical care operations, Hospital Pavia Arecibo may also use the patient's PHI for the following purposes:

-
    1. **Business Associates:** We may hire third parties to provide us with certain types of services. For example, we can use these services from transcription and collection companies. With such agreements, we can exchange your information to perform the work we have contracted. Likewise, these types of business associate agreements require these entities to protect the medical information we provide. Business partners may receive, create, maintain, use and disclose PHI, only after obtaining a legal agreement with Hospital Pavia Arecibo that establishes the business partner relationship and its obligations to comply with the provisions of HIPAA (45 CFR Part 160 and 164).
    2. **Appointment Reminders:** We can contact you to remind you of your medical appointments.
    3. **Health promotion information and activities**: Hospital Pavia Arecibo may use and disclose some of the patient's PHI for certain health promotion activities. For example, the patient's name and address will be used to send you a general newsletter or specific information related to their own health interests.
    4. **Treatment Alternatives:** We may use and disclose your medical information to inform you of or recommend possible treatment options or alternatives that may be of interest to you.
    5. **Medical Research.** We may share your medical information with medical researchers who request it for medical research projects approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your medical information. We may also use and share your

medical information to contact you about the possibility of enrolling in a research study. Researchers are required to protect all the PHI information they receive.

6. **Fundraising Notices:** We may use your medical information to contact you in an effort to raise money for our hospital or clinic. For example, we can send you a letter asking if you would like to make a donation. You can choose not to contact us for our collection efforts. If we send you information about our collection efforts, we will include a simple way for you to ask us not to contact you in the future for our collection efforts.
7. **Genetic Information:** Hospital Pavia Arecibo may not use or disclose genetic information for risk analysis purposes. However, we may use genetic information, for example, to determine medical necessity when you request a benefit under the plan or coverage.

II. Use or Disclosure that Require us to Give the Patient an Opportunity to Accept or Object

A. **Persons involved in your care:** Unless you object, we may provide your medical information to a friend or family member who is involved in your care. The information disclosed may include information that we consider directly relevant for participation in your care, your location, your overall condition or your death. Should you not be aware or in the event of an emergency, we will disclose your medical information if we determine it is in your best interest. We may also disclose your medical information to humanitarian organizations authorized to handle disaster relief, so that those who care about you can receive information about your location or health condition.

B. **Hospital Directory:** We may include certain limited information about you in the hospital directory while you are in the hospital. This information may include your name, your location in the hospital, your general medical condition (regular, stable, etc.) and your religious affiliation. We may disclose information from the directory, excluding religion, to those people who ask for you by giving your full name. Information related to your religious affiliation may be disclosed to clergy members. This service is designed so that your family, friends and clergy can visit you at the hospital and to know how you are doing. Should you not want anyone to know about your hospital admission, we will not disclose any information. You will have to inform the Hospital Admissions Department if you do not want this information to be disclosed.

C. **Spiritual Care:** The information on the directory, including the patient's religious affiliation, will be given to a member of the clergy, even if they do not ask for their name. Spiritual care providers are members of Hospital Pavia Arecibo health care team who may be asked about the patient’s care. The patient is entitled to request that their name not be given to any member of the clergy.

III. Use or Disclosure that Requires Patient Authorization

Any other use of medical information that has not been mentioned in this notice or by other laws that concern us, will be made only with your written authorization. The following is a description of some, but not all, situations in which the use and disclosure of your medical information by us will require your written authorization:

A. **Marketing:** Subject to limited exceptions, the patient's written authorization is required in those cases in which Hospital Pavia Arecibo receives a direct or indirect remuneration in exchange for disclosing PHI to another entity in order to market the product or service to the patient.
B. **Research:** Hospital Pavia Arecibo will obtain the patient's written authorization to use or disclose PHI for research purposes when required by HIPAA.
C. **Notes on Psychotherapy:** With limited exceptions, psychotherapy notes will not be disclosed without the express authorization of the patient.
D. **Sale of PHI:** Sale of PHI, which involves disclosure of PHI by a covered entity or business partner in exchange for direct or indirect remuneration. You are entitled to revoke it in writing at any time, pursuant to Section 164.508(b)(5) of the Privacy Regulation. The revocation will be in effect for future uses and disclosures of your PHI and will not affect the uses and disclosures allowed by your authorization while it was in force. Unless you send us a written authorization, we may not use or disclose your PHI for any other reason that is not described in this Notice.
E. **Other Uses and Disclosures:** Any other use or disclosure of PHI that is not described in this Notice of Privacy Practices requires the patient's written authorization. Written authorizations will let the patient know why PHI is being used.

IV. Should you authorize us to use or share your medical information, you may terminate this permission in writing at any time. If you decide to terminate this permission, we will not use or share your medical information, thus following the reasons described in your written request. On the other hand, we cannot retract any information that we have given in the past with your authorization. We are required to keep a record of the care we have provided to you.

V. Use or Disclosure Permitted or Required by Public Policy or Law Without Patient Authorization

A. **Lawsuits and Litigation.** If you are involved in a lawsuit or litigation, we may disclose your information in response to a court order, a lawsuit or other legal process.
B. **Law Enforcement Agency.** We may transfer your medical information to a law enforcement agent if so required to:
    1. Report certain types of wounds.
    2. In response to a court order, subpoena, arrest warrant, or other similar proceeding.
    3. To identify or locate a suspect, a fugitive, a material witness, or a missing person.
    4. In certain circumstances, in order to give information about a crime victim in case of not being able to obtain the consent of the victim.
    5. To report the cause of a death we believe has been caused by criminal conduct.

6. To report suspicious criminal behavior within our facilities.
7. In case of an emergency, to report a crime, the place of the crime or the victims or their identity, description or place where the person who committed the crime is located.

Abuse, Neglect or Domestic Violence: We may notify designated government authorities, including social services or protective services agencies, if there is a reasonable belief that a patient is a victim of abuse, neglect or domestic violence. We will make such disclosure to the extent that it is expressly authorized by law or when the patient agrees to such disclosure.

Public Health Risks. As required by law, we may disclose your medical information for public health issues, such as:

0. To control or prevent illness, injury or disability.
1. To report vital events of births or deaths.
2. To report child negligence or abuse to designated government authorities.
3. To provide information about products or services within the jurisdiction of the United States Food and Drug Administration.
4. To notify you if you have been exposed to any disease or if you could run the risk of contracting or spreading a disease or condition.
5. To provide information to your employer, as required by laws dealing with occupational diseases and injuries or workplace safety.

Prosecutors, Forensic Pathologists and Funeral Directors. We may disclose your medical information to a prosecutor, or a forensic pathologist. For example, this will be necessary to identify a deceased or to determine a cause of death. We may also share your medical information to funeral directors as necessary to carry out their duties.

Organ and Tissue Donation. We may share your medical information with organizations that handle or control organ donations and transplants.

Military and Veterans of the Armed Forces. If you are a member of the armed forces of the U.S. or another country, we may share your medical information as required by the military commanding officers.

Work Compensation. We may disclose your medical information for workers' compensation or similar programs. We will do this to the extent required by the law.

Health Oversight Activities: We may disclose medical information to government health oversight agencies, such as the Puerto Rico Department of Health, for activities authorized by law. These activities include: audits, investigations, inspections and licenses. The government makes use of these activities in order to monitor the health system, government programs and compliance with civil rights laws.

National Security. We may transfer your medical information to authorized federal agents for national security purposes.

Student Immunization Records: Hospital Pavia Arecibo may disclose evidence of immunization to a school if the law requires the school to have such evidence prior to the student's admission and document the authorization of disclosure by the parent, guardian and/or legal guardian of the minor, or of the individual if he/she is an adult or an emancipated minor.

Prisoners: If you are an inmate of a correctional institution or under the custody of a law enforcement officer, we may disclose your medical information to the correctional officer or law enforcement officer. This disclosure may be necessary for the

institution to provide you with health care; protect your health and safety or the health and safety of others; or for the security and guarantee of the correctional institution.

As required by law: We may disclose your medical information when so required by federal or state law.

Patient's Medical Information Rights

You have the following rights regarding your medical information:

. **Right of access to information and receive copies thereof:** You have the right to inspect and request copies of medical information that has been used to make decisions about your health. To review or obtain copies of your medical information, you must make a written request to the Hospital Health Information Management Department. You will be charged a reasonable fee for copies of your medical information, in accordance with applicable federal or state law. You will also be entitled to request your health information in electronic format, if it can be produced in that format; otherwise, you will be physically provided a ¨hard copy¨. If the copies provided are in electronic format, you will only be charged for labor costs. For more information, please call the Hospital Health Information Management Department. In certain situations you may be denied access to medical information (for example, mental health records or information collected for legal proceedings), as provided by law. In such a case, you may request that your case be reviewed, so please contact the Hospital Information Management Department.

A. **Right to Amend:** You are entitled to request an amendment regarding your protected health information or your medical record. To do this, you must fill out a written request and submit it to the Hospital Health Information Management Department. You must also include the reason for submitting the request. We may deny the request if it has not been submitted in writing or for not attaching the reason for it. We may also deny your request for amendment if:

1. It was not created by us.
2. The information is not part of the designated record set.
3. The information would not be available for patient inspection (due to its condition or nature).
4. The information is accurate and complete.

If **Hospital Pavia Arecibo** denies the patient the request to change the PHI, the patient will be notified in writing with the reason for the denial. Hospital Pavia Arecibo will also inform the patient of their right to submit a written statement expressing their disagreement with the denial. The patient may request that the request for amendment and the denial be included each time the information they wanted to amend is subsequently disclosed. Hospital Pavia Arecibo may prepare the rebuttal to the patient's

statement of disagreement and will provide the patient with a copy of said rebuttal.

B. **Right to obtain a detail of the disclosures:** The patient is entitled to obtain a list of disclosures of PHI that the Hospital made, except in the following situations: treatment, payment or medical care operations; patient disclosure; disclosure to people involved in patient care; for national security or intelligence purposes; or to prisons or law enforcement officers. The patient must submit the request for the list of disclosures of the PHI in writing to the Hospital. The patient must include the period of detail that cannot exceed 6 years. In a given period of 12 months, the Hospital will provide the patient with the detail of the disclosures of PHI free of charge. Any additional request for detail within that period of time will be subject to the application of a reasonable sum to prepare said detail.

C. **Right to Request Restrictions.** You are entitled to request that medical information that is disclosed for treatment, payments or health care operations be restricted or limited. You may also request that the medical information we disclose be restricted, if it is for the purposes of medical insurance policies or payments (not for the purposes of health care operations) and if the medical information belongs only to a health service for which you have already paid out of pocket in full. You may also be entitled to restrict the information we share with those who are involved in your care or in paying for it. These people could be a family member or friend. On the contrary, we reserve the right to refuse your request. If we approve the request, we will comply with your request unless this information is necessary to be able to provide you with emergency treatment. This request must be submitted in writing by filling out a form which will be delivered to you at any time. You must add:
    1. What type of information do you want to restrict?
    2. How do you want us to restrict it?
    3. To whom you want the restrictions to be applied?

D. **Right to Request Confidential Communications:** You are entitled to request that we communicate with you in a particular way or place when referring to medical matters. For example, the patient may request that the Hospital only contact them at work or by email. This request must be submitted in writing by filling out a form that will be delivered to them whenever they wish. We will accept all requests that are reasonable.

E. **Right to Receive a Copy of this Notice:** You may request that we give you a copy of this notice at any time. Even if you have already requested a copy in electronic format.

F. **Rights Concerning the Electronic Exchange of Health Information**
Once we have the electronic record, we will be able to participate in the electronic exchange of health information with other medical professionals and health plans through an approved

Health Information Organization (HIO). Through our participation, other medical professionals and health plans will be able to access your PHI for treatment, payment or health care operations. The approved HIO is required to maintain safeguards to protect the privacy and security of PHI. The approved agency will only allow authorized personnel access through its agency. You are entitled to decide whether medical professionals and health plans can access your health information through this agency. You have two options. The first is that it can allow authorized persons access to your PHI maintained through an agency for treatment, payment, or health care operations. If you choose this option, you do not have to do anything.
The second is that you can restrict access to your PHI. To do so, you must submit a written request for exclusion and restriction. You can apply for it at the Admissions Department or at the Hospital Health Information Management Department. Even if you restrict access to your PHI, medical professionals and health plans may share your information through other legal means already available without your specific authorization.
Understand that your decision to restrict access to your electronic health information may limit the ability of your health care providers to provide you with the most effective care. When submitting a restriction request, you accept the risks associated with that decision.

Violation of PHI information

In compliance with the law, we will keep your medical information private and secure. If someone acquires, accesses, uses or transfers a portion of your medical information in a manner not permitted by law, we will notify you within 60 days of discovery.

Changes to this Notice

Hospital Pavia Arecibo will abide by the terms of this Notice currently in force. Hospital Pavia Arecibo reserves the right to make substantial changes to the terms of this Notice and to enforce new provisions of the Notice regarding all PHI it maintains. Hospital Pavia Arecibo will provide the patient with the amended Notice on the first visit of the one that is subsequent to the amendment of the Notice in cases where there is a substantial change therein. The patient may also request an updated copy of the Notice from the Hospital at any time.

Complaints

If the patient considers that their privacy rights have been violated, they may file a complaint with the Hospital Compliance Officer or with the Secretary of the Department of Health. All complaints must be submitted in writing directly to the Hospital Compliance Officer. The Hospital ensures that the patient will not be subject to retaliation for filing a complaint.

Questions, concerns or additional information

Should the patient have any questions, concerns or want further information regarding the issues covered by this Notice of Privacy Practices or seek additional information regarding the privacy policies and procedures of Hospital Pavia Arecibo, they must contact the Director of Corporate Compliance on the hotline free of charge at 1-888-882-0882, or e-mail compliance@metropaviahealth.com. You may write to Metro Pavía Health System, Maramar, Plaza Building 101, San Patricio Ave. Suite 950-960 Guaynabo, PR, 00968 OR CALL 787-999-8944.

HIPAA

Effective Date: April 14, 2003
Effective amendment date: April 14, 2003
Review date: September 23, 2013

THIS NOTICE DESCRIBES HOW THE PATIENT'S MEDICAL INFORMATION MAY BE USED AND DISCLOSED AND HOW THEY CAN GET ACCESS TO THIS INFORMATION. PLEASE READ THE CONTENT CAREFULLY.

The Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act (found in Title XIII of the American Recovery and Reinvestment Act of 2009) (collectively referred to as "HIPAA"), with the amendments that are implemented in a timely manner, require that Hospital Pavia Santurce maintain the privacy of individually identifiable patient health information (this information is considered "protected health information" and is referred to herein as "PHI"). The HIPAA Privacy Rule requires that we provide a detailed written notice about our privacy practices.

Hospital Pavia Santurce understands that the patient's health information is exclusively personal and we undertake to protect] the patient's privacy. Read this Notice of Privacy Practices carefully. This notice informs you of how we may use your medical information and/or disclose it to third parties. It also describes your rights and certain obligations we have regarding the use and disclosure of medical information.

According to the law, we must:

1. Be sure to maintain the privacy of medical information that identifies you.
2. Give you this notice about our legal duties and privacy practices regarding your medical information.
3. Comply with the terms of this notice that are currently in effect.

This Notice applies to the provision of health care by Hospital Pavia Santurce, medical staff, outpatient departments and clinics. This Notice also applies to the utilization review and quality assessment activities of Hospital Pavia Santurce.

I. Permitted Use or Disclosure

The following sections describe different ways that we are authorized to use and disclose your medical information. Not all categories are mentioned, however, all those in which we are allowed to use and/or disclose your information to others, are derived from one of the following categories:

A. **For Treatment:** We may use medical information about you to provide you with medical treatment. We may also exchange it with doctors, nurses, technicians, students, or other staff members, such as the departments of the Hospital may share your medical information to coordinate elements of your care, such as prescriptions, blood tests and x-rays. We may also exchange your medical information with people

outside **Hospital Pavia Santurce**, such as with the doctors who referred you and with those who treat you.

B. **For Payment:** We may use your information and/or transfer it to your health insurance policy or to other people who help you pay for your care. For example, we may inform your health insurance about a treatment you are going to receive to determine if your health care insurance would pay for that treatment.

C. **For Health Care Operations:** We may use your medical information to improve the quality of care we provide. These activities help us carry out our programs to ensure that all our patients receive quality health care. For example, we may use your information to review our treatments and services. Also, to evaluate the effectiveness of our employees and their care for you. We may also disclose your health information to doctors, nurses, technicians, students, and other health care employees for educational purposes or as preparation for research.

D. **Other Uses and Disclosures:** As part of the treatment, payment and medical care operations, Hospital Pavia Santurce may also use the patient's PHI for the following purposes:

-

1. **Business Associates:** We may hire third parties to provide us with certain types of services. For example, we can use these services from transcription and collection companies. With such agreements, we can exchange your information to perform the work we have contracted. Likewise, these types of business associate agreements require these entities to protect the medical information we provide. Business partners may receive, create, maintain, use and disclose PHI, only after obtaining a legal agreement with Hospital Pavia Santurce that establishes the business partner relationship and its obligations to comply with the provisions of HIPAA (45 CFR Part 160 and 164).
2. **Appointment Reminders:** We can contact you to remind you of your medical appointments.
3. **Health promotion information and activities**: Hospital Pavia Santurce may use and disclose some of the patient's PHI for certain health promotion activities. For example, the patient's name and address will be used to send you a general newsletter or specific information related to their own health interests.
4. **Treatment Alternatives:** We may use and disclose your medical information to inform you of or recommend possible treatment options or alternatives that may be of interest to you.
5. **Medical Research.** We may share your medical information with medical researchers who request it for medical research projects approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your medical information. We may also use and share your

medical information to contact you about the possibility of enrolling in a research study. Researchers are required to protect all the PHI information they receive.

6. **Fundraising Notices:** We may use your medical information to contact you in an effort to raise money for our hospital or clinic. For example, we can send you a letter asking if you would like to make a donation. You can choose not to contact us for our collection efforts. If we send you information about our collection efforts, we will include a simple way for you to ask us not to contact you in the future for our collection efforts.
7. **Genetic Information:** Hospital Pavia Santurce may not use or disclose genetic information for risk analysis purposes. However, we may use genetic information, for example, to determine medical necessity when you request a benefit under the plan or coverage.

II. Use or Disclosure that Require us to Give the Patient an Opportunity to Accept or Object

A. **Persons involved in your care:** Unless you object, we may provide your medical information to a friend or family member who is involved in your care. The information disclosed may include information that we consider directly relevant for participation in your care, your location, your overall condition or your death. Should you not be aware or in the event of an emergency, we will disclose your medical information if we determine it is in your best interest. We may also disclose your medical information to humanitarian organizations authorized to handle disaster relief, so that those who care about you can receive information about your location or health condition.

B. **Hospital Directory:** We may include certain limited information about you in the hospital directory while you are in the hospital. This information may include your name, your location in the hospital, your general medical condition (regular, stable, etc.) and your religious affiliation. We may disclose information from the directory, excluding religion, to those people who ask for you by giving your full name. Information related to your religious affiliation may be disclosed to clergy members. This service is designed so that your family, friends and clergy can visit you at the hospital and to know how you are doing. Should you not want anyone to know about your hospital admission, we will not disclose any information. You will have to inform the Hospital Admissions Department if you do not want this information to be disclosed.

C. **Spiritual Care:** The information on the directory, including the patient's religious affiliation, will be given to a member of the clergy, even if they do not ask for their name. Spiritual care providers are members of Hospital Pavia Santurce health care team who may be asked about the patient’s care. The patient is entitled to request that their name not be given to any member of the clergy.

III. Use or Disclosure that Requires Patient Authorization

Any other use of medical information that has not been mentioned in this notice or by other laws that concern us, will be made only with your written authorization. The following is a description of some, but not all, situations in which the use and disclosure of your medical information by us will require your written authorization:

A. **Marketing:** Subject to limited exceptions, the patient's written authorization is required in those cases in which Hospital Pavia Santurce receives a direct or indirect remuneration in exchange for disclosing PHI to another entity in order to market the product or service to the patient.
B. **Research:** Hospital Pavia Santurce will obtain the patient's written authorization to use or disclose PHI for research purposes when required by HIPAA.
C. **Notes on Psychotherapy:** With limited exceptions, psychotherapy notes will not be disclosed without the express authorization of the patient.
D. **Sale of PHI:** Sale of PHI, which involves disclosure of PHI by a covered entity or business partner in exchange for direct or indirect remuneration. You are entitled to revoke it in writing at any time, pursuant to Section 164.508(b)(5) of the Privacy Regulation. The revocation will be in effect for future uses and disclosures of your PHI and will not affect the uses and disclosures allowed by your authorization while it was in force. Unless you send us a written authorization, we may not use or disclose your PHI for any other reason that is not described in this Notice.
E. **Other Uses and Disclosures:** Any other use or disclosure of PHI that is not described in this Notice of Privacy Practices requires the patient's written authorization. Written authorizations will let the patient know why PHI is being used.

IV. Should you authorize us to use or share your medical information, you may terminate this permission in writing at any time. If you decide to terminate this permission, we will not use or share your medical information, thus following the reasons described in your written request. On the other hand, we cannot retract any information that we have given in the past with your authorization. We are required to keep a record of the care we have provided to you.

V. Use or Disclosure Permitted or Required by Public Policy or Law Without Patient Authorization

A. **Lawsuits and Litigation.** If you are involved in a lawsuit or litigation, we may disclose your information in response to a court order, a lawsuit or other legal process.
B. **Law Enforcement Agency.** We may transfer your medical information to a law enforcement agent if so required to:
    1. Report certain types of wounds.
    2. In response to a court order, subpoena, arrest warrant, or other similar proceeding.
    3. To identify or locate a suspect, a fugitive, a material witness, or a missing person.
    4. In certain circumstances, in order to give information about a crime victim in case of not being able to obtain the consent of the victim.
    5. To report the cause of a death we believe has been caused by criminal conduct.

6. To report suspicious criminal behavior within our facilities.
7. In case of an emergency, to report a crime, the place of the crime or the victims or their identity, description or place where the person who committed the crime is located.

Abuse, Neglect or Domestic Violence: We may notify designated government authorities, including social services or protective services agencies, if there is a reasonable belief that a patient is a victim of abuse, neglect or domestic violence. We will make such disclosure to the extent that it is expressly authorized by law or when the patient agrees to such disclosure.

Public Health Risks. As required by law, we may disclose your medical information for public health issues, such as:

0. To control or prevent illness, injury or disability.
1. To report vital events of births or deaths.
2. To report child negligence or abuse to designated government authorities.
3. To provide information about products or services within the jurisdiction of the United States Food and Drug Administration.
4. To notify you if you have been exposed to any disease or if you could run the risk of contracting or spreading a disease or condition.
5. To provide information to your employer, as required by laws dealing with occupational diseases and injuries or workplace safety.

Prosecutors, Forensic Pathologists and Funeral Directors. We may disclose your medical information to a prosecutor, or a forensic pathologist. For example, this will be necessary to identify a deceased or to determine a cause of death. We may also share your medical information to funeral directors as necessary to carry out their duties.

Organ and Tissue Donation. We may share your medical information with organizations that handle or control organ donations and transplants.

Military and Veterans of the Armed Forces. If you are a member of the armed forces of the U.S. or another country, we may share your medical information as required by the military commanding officers.

Work Compensation. We may disclose your medical information for workers' compensation or similar programs. We will do this to the extent required by the law.

Health Oversight Activities: We may disclose medical information to government health oversight agencies, such as the Puerto Rico Department of Health, for activities authorized by law. These activities include: audits, investigations, inspections and licenses. The government makes use of these activities in order to monitor the health system, government programs and compliance with civil rights laws.

National Security. We may transfer your medical information to authorized federal agents for national security purposes.

Student Immunization Records: Hospital Pavia Santurce may disclose evidence of immunization to a school if the law requires the school to have such evidence prior to the student's admission and document the authorization of disclosure by the parent, guardian and/or legal guardian of the minor, or of the individual if he/she is an adult or an emancipated minor.

Prisoners: If you are an inmate of a correctional institution or under the custody of a law enforcement officer, we may disclose your medical information to the correctional officer or law enforcement officer. This disclosure may be necessary for the

institution to provide you with health care; protect your health and safety or the health and safety of others; or for the security and guarantee of the correctional institution.

As required by law: We may disclose your medical information when so required by federal or state law.

Patient's Medical Information Rights

You have the following rights regarding your medical information:

. **Right of access to information and receive copies thereof:** You have the right to inspect and request copies of medical information that has been used to make decisions about your health. To review or obtain copies of your medical information, you must make a written request to the Hospital Health Information Management Department. You will be charged a reasonable fee for copies of your medical information, in accordance with applicable federal or state law. You will also be entitled to request your health information in electronic format, if it can be produced in that format; otherwise, you will be physically provided a ¨hard copy¨. If the copies provided are in electronic format, you will only be charged for labor costs. For more information, please call the Hospital Health Information Management Department. In certain situations you may be denied access to medical information (for example, mental health records or information collected for legal proceedings), as provided by law. In such a case, you may request that your case be reviewed, so please contact the Hospital Information Management Department.

A. **Right to Amend:** You are entitled to request an amendment regarding your protected health information or your medical record. To do this, you must fill out a written request and submit it to the Hospital Health Information Management Department. You must also include the reason for submitting the request. We may deny the request if it has not been submitted in writing or for not attaching the reason for it. We may also deny your request for amendment if:

1. It was not created by us.
2. The information is not part of the designated record set.
3. The information would not be available for patient inspection (due to its condition or nature).
4. The information is accurate and complete.

If **Hospital Pavia Santurce** denies the patient the request to change the PHI, the patient will be notified in writing with the reason for the denial. Hospital Pavia Santurce will also inform the patient of their right to submit a written statement expressing their disagreement with the denial. The patient may request that the request for amendment and the denial be included each time the information they wanted to amend is subsequently disclosed. Hospital Pavia Santurce may prepare the rebuttal to the patient's

statement of disagreement and will provide the patient with a copy of said rebuttal.

B. **Right to obtain a detail of the disclosures:** The patient is entitled to obtain a list of disclosures of PHI that the Hospital made, except in the following situations: treatment, payment or medical care operations; patient disclosure; disclosure to people involved in patient care; for national security or intelligence purposes; or to prisons or law enforcement officers. The patient must submit the request for the list of disclosures of the PHI in writing to the Hospital. The patient must include the period of detail that cannot exceed 6 years. In a given period of 12 months, the Hospital will provide the patient with the detail of the disclosures of PHI free of charge. Any additional request for detail within that period of time will be subject to the application of a reasonable sum to prepare said detail.

C. **Right to Request Restrictions.** You are entitled to request that medical information that is disclosed for treatment, payments or health care operations be restricted or limited. You may also request that the medical information we disclose be restricted, if it is for the purposes of medical insurance policies or payments (not for the purposes of health care operations) and if the medical information belongs only to a health service for which you have already paid out of pocket in full. You may also be entitled to restrict the information we share with those who are involved in your care or in paying for it. These people could be a family member or friend. On the contrary, we reserve the right to refuse your request. If we approve the request, we will comply with your request unless this information is necessary to be able to provide you with emergency treatment. This request must be submitted in writing by filling out a form which will be delivered to you at any time. You must add:
    1. What type of information do you want to restrict?
    2. How do you want us to restrict it?
    3. To whom you want the restrictions to be applied?

D. **Right to Request Confidential Communications:** You are entitled to request that we communicate with you in a particular way or place when referring to medical matters. For example, the patient may request that the Hospital only contact them at work or by email. This request must be submitted in writing by filling out a form that will be delivered to them whenever they wish. We will accept all requests that are reasonable.

E. **Right to Receive a Copy of this Notice:** You may request that we give you a copy of this notice at any time. Even if you have already requested a copy in electronic format.

F. **Rights Concerning the Electronic Exchange of Health Information**
Once we have the electronic record, we will be able to participate in the electronic exchange of health information with other medical professionals and health plans through an approved

Health Information Organization (HIO). Through our participation, other medical professionals and health plans will be able to access your PHI for treatment, payment or health care operations. The approved HIO is required to maintain safeguards to protect the privacy and security of PHI. The approved agency will only allow authorized personnel access through its agency. You are entitled to decide whether medical professionals and health plans can access your health information through this agency. You have two options. The first is that it can allow authorized persons access to your PHI maintained through an agency for treatment, payment, or health care operations. If you choose this option, you do not have to do anything.
The second is that you can restrict access to your PHI. To do so, you must submit a written request for exclusion and restriction. You can apply for it at the Admissions Department or at the Hospital Health Information Management Department. Even if you restrict access to your PHI, medical professionals and health plans may share your information through other legal means already available without your specific authorization.
Understand that your decision to restrict access to your electronic health information may limit the ability of your health care providers to provide you with the most effective care. When submitting a restriction request, you accept the risks associated with that decision.

Violation of PHI information

In compliance with the law, we will keep your medical information private and secure. If someone acquires, accesses, uses or transfers a portion of your medical information in a manner not permitted by law, we will notify you within 60 days of discovery.

Changes to this Notice

Hospital Pavia Santurce will abide by the terms of this Notice currently in force. Hospital Pavia Santurce reserves the right to make substantial changes to the terms of this Notice and to enforce new provisions of the Notice regarding all PHI it maintains. Hospital Pavia Santurce will provide the patient with the amended Notice on the first visit of the one that is subsequent to the amendment of the Notice in cases where there is a substantial change therein. The patient may also request an updated copy of the Notice from the Hospital at any time.

Complaints

If the patient considers that their privacy rights have been violated, they may file a complaint with the Hospital Compliance Officer or with the Secretary of the Department of Health. All complaints must be submitted in writing directly to the Hospital Compliance Officer. The Hospital ensures that the patient will not be subject to retaliation for filing a complaint.

Questions, concerns or additional information

Should the patient have any questions, concerns or want further information regarding the issues covered by this Notice of Privacy Practices or seek additional information regarding the privacy policies and procedures of Hospital Pavia Santurce, they must contact the Director of Corporate Compliance on the hotline free of charge at 1-888-882-0882, or e-mail compliance@metropaviahealth.com. You may write to Metro Pavía Health System, Maramar, Plaza Building 101, San Patricio Ave. Suite 950-960 Guaynabo, PR, 00968 OR CALL 787-999-8944.

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): Indiano, David C.

USDC-PR Bar Number: 200601

Email Address: david.indiano@indianowilliams.com

---

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

   Plaintiff: Pablo J. Quintero

   Defendant: Metro Santurce, 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).

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: February 11, 2020

rev. Dec. 2009

Print Form Reset Form

JS 44 (Rev. 06/17)

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

PABLO J. QUINTERO, and JOANNIE PRINCIPE, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Guaynabo, Puerto Rico
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Indiano & Williams, P.S.C.
207 Del Parque Street, Third Floor, San Juan, PR 00912
787-641-4545

DEFENDANTS

METRO SANTURCE, INC., d/b/a PAVIA HOSPITAL SANTURCE a corporation, METRO HATO REY, INC., d/b/ a PAVIA HOSPITAL HATO REY and DOES 1 to 10, inclusive

County of Residence of First Listed Defendant Puerto Rico
(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
- ❒ 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:
Breach of Express And/or Implied Contractual Promise, Breach of Covenant of Good Faith and Fair Dealing, Negli

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE _____ DOCKET NUMBER _____

DATE
February 11, 2020

SIGNATURE OF ATTORNEY OF RECORD
s/David C. Indiano

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

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

UNITED STATES DISTRICT COURT

for the

District of Puerto Rico

PABLO J. QUINTERO, and JOANNIE PRINCI

Plaintiff(s)

v.

METRO SANTURCE, INC., d/b/a PAVIA HOS

Defendant(s)

Civil Action No. 20-cv-01075

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

METRO SANTURCE, INC. d/b/a PAVIA HOSPITAL SANTURCE

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) — or 90 days in a Social Security Action — 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:

DAVID C. INDIANO, ESQ.

Indiano & Williams, P.S.C., 207 Del Parque Street, 3rd Floor San Juan, P.R. 00912

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.

FRANCES RIOS DE MORAN, ESQ.
CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

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)* _____ 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 $ _____ .

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:

_____

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

UNITED STATES DISTRICT COURT

for the

District of Puerto Rico

PABLO J. QUINTERO, and JOANNIE PRINCI

Plaintiff(s)

v.

METRO SANTURCE, INC., d/b/a PAVIA HOS

Defendant(s)

Civil Action No. 20-cv-01075

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

METRO HATO REY, INC., d/b/a PAVIA HOSPITAL HATO REY

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) — or 90 days in a Social Security Action — 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:

DAVID C. INDIANO, ESQ.

Indiano & Williams, P.S.C., 207 Del Parque Street, 3rd Floor San Juan, P.R. 00912

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.

FRANCES RIOS DE MORAN, ESQ.
CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

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)* _____ 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 $ _____ .

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:

_____