Teague Westrope
Kasodie West
AVA Law Group, PLLC
2718 Montana Ave., Suite 220
Billings, MT 59101
(406) 295-8689
teague.westrope@avalaw.com
kasodie.west@avalaw.com

Leigh S. Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEYS FOR PLAINTIFF
(* denotes *pro hac vice* forthcoming)

MONTANA THIRTEENTH JUDICIAL DISTRICT
COUNTY OF YELLOWSTONE

SARAH SULLIVAN, individually, on behalf of her minor child, M.S., and on behalf of all others similarly situated, Plaintiff, v. INTERMOUNTAIN PLANNED PARENTHOOD, INC., d/b/a PLANNED PARENTHOOD OF MONTANA, Defendant	**Case No:** DV-56-2024-0001408-PI Jessica T. Fehr **COMPLAINT – CLASS ACTION** **DEMAND FOR JURY TRIAL**

PLAINTIFF'S ORIGINAL CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff Sarah Sullivan ("Plaintiff"), individually, on behalf of her minor child, M.S., and on behalf of all others similarly situated, sues Intermountain Planned Parenthood, Inc., d/b/a Planned Parenthood of Montana ("Planned Parenthood" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiff and other current and former patients of Defendant, the putative class members ("Class"). This Data Breach occurred on or between August 24 and 28, 2024.

2. The Private Information compromised in the Data Breach included certain personal or protected health information of Defendant Planned Parenthood's patients, including Plaintiff's minor child. This Private Information included but is not limited to "name, address, date of birth, medical record number, health insurance information, provider name(s), date(s) of service, diagnosis information, treatment information, and/or prescription information."[1]

3. The Private Information was exposed to cybercriminals who perpetrated the attack and remains in the hands of those cybercriminals. According to Defendant's report to the U.S. Department of Health and Human Services, 18,003 individuals' sensitive data was compromised.[2]

[1] Planned Parenthood Notice Letter, *available at* https://dojmt.gov/wp-content/uploads/2024/11/Consumer-notification-letter-30.pdf (*last accessed* Nov. 15, 2024).
[2] U.S. Department of Health & Human Services Office for Civil Rights, *Cases Currently Under Investigation*, (November 5, 2024), *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (*last accessed* Nov. 15, 2024).

4. A cybercriminal group called RansomHub claimed responsibility for the Data Breach.[3]

5. The Data Breach resulted from Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which they were entrusted for treatment.

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what type of information was accessed.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. Defendant, through its employees, disregarded the rights of Plaintiff and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class

[3] Jill McKeon, "RansomHub claims Planned Parenthood cyberattack," *available at* https://www.techtarget.com/healthtechsecurity/news/366609974/RansomHub-claims-Planned-Parenthood-cyberattack (*last accessed* Nov. 17, 2024).

Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

9. In addition, Defendant's employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

10. Plaintiff's and Class Members' identities and privacy are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. Because of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

16. Accordingly, Plaintiff sues Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract, (iii) negligence *per se*, and (iv) breach of fiduciary duty.

II. PARTIES

17. Plaintiff Sarah Sullivan is and at all times mentioned herein was an individual citizen of Montana, residing in the city of South Great Falls.

18. Plaintiff Sullivan provided Defendant with her sensitive PII and the sensitive PII and PHI of M.S., Plaintiff's minor child, to receive healthcare services for M.S. from Defendant. Plaintiff received notice of the Data Breach around November 5, 2024, informing her that M.S.'s sensitive information was part of Defendant's Data Breach.

19. Defendant Intermountain Planned Parenthood, Inc., d/b/a Planned Parenthood of Montana is a Montana non-profit corporation with its principal place of business at 1643 Lewis Avenue, Suite 211, Billings, Montana, 59102.

20. Defendant's registered agent is Martha Fuller, located at 1643 Lewis Avenue, Suite 211, Billings, Montana, 59102.

III. JURISDICTION AND VENUE

21. This Court has original jurisdiction over this action pursuant to Article VII, § 4 of the Montana Constitution and M.C.A. § 3-5-302.

22. This Court has general personal jurisdiction over Defendant pursuant to M.C.A. § 25-20-4 because Planned Parenthood has its principal place of business in Montana and the acts and omissions complained of occurred within this state.

23. Venue is proper in this Court pursuant to M.C.A. § 25-20-4 because Defendant has its principal place of business in Yellowstone County.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

24. Defendant is a healthcare provider that operates five health centers in Montana.

25. In the ordinary course of receiving health care services from Defendant, each client must provide (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as his or her:

- address;
- telephone number;
- date of birth;
- health insurance information; and
- medical history.

26. All of Defendant's employees, staff, entities, sites, and locations may share patient information with each other for various purposes, as should be disclosed in a HIPAA compliant privacy notice ("Privacy Policy") that Defendant is required to maintain.

27. Upon information and belief, Defendant's HIPAA Privacy Policy is provided to every patient prior to receiving treatment and upon request.

28. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in

compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

29. The patient information held by Defendant in its computer system and network included the Private Information of Plaintiff and Class Members.

THE DATA BREACH

30. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

31. According to the notice letter Defendant provided to the Montana Department of Justice,

> ***What Happened?***
> On August 28, 2024, PPMT learned that some of our systems were subject to unauthorized access. We immediately took steps to secure our systems, began an investigation with the assistance of cybersecurity partners, and notified law enforcement. On September 6, 2024, we determined that an unauthorized person gained access to our network and acquired certain files that contained patient information. The files were acquired between August 24, 2024 and August 28, 2024.
>
> ***What Information Was Involved?***
> We reviewed the documents involved and determined that one or more files may have contained your information, which may have included your name, address, date of birth, medical record number, health insurance information, provider name(s), date(s) of service, diagnosis information, treatment information, and/or prescription information.

32. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[4] Further, if "the number of individuals affected by a breach

[4] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed September 5, 2024) (emphasis added).

is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HHS.[5]

33. Defendant cannot claim it was unaware of the HHS notification requirements as it complied (at least in part) with those requirements.

34. Defendant's notice to HHS was dated November 5, 2024—around ten weeks after the incident was discovered.

35. Defendant had obligations created by HIPAA, contract, industry standards, state statutes, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

36. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

37. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in the healthcare industry preceding the date of the breach.

38. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[6] Of the 2023 recorded data breaches, 809 of them, or 25%, were in the medical or healthcare industry.[7] The 809 reported breaches reported in 2023 exposed nearly 56 million sensitive records, compared to only 343 breaches that exposed just over 28 million sensitive records in 2022.[8]

---

[5] *Id.*
[6] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited June 10, 2024).
[7] *Id*.
[8] *Id*. at 11, Fig.3.

39. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

40. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in one year's time.[9]

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

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

42. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

43. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient 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 any security problems.[10] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting

[9] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), *available at* https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited May 21, 2024).

[10] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 19, 2024).

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.[11]

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

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

46. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

47. Defendant failed to properly implement basic data security practices.

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

[11] *Id*.

49. Defendant was always fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

50. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

51. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including, but not limited to, educating all employees; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

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

53. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, without limitation, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

54. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANT'S CONDUCT VIOLATES HIPAA AND REVEALS ITS INSUFFICIENT DATA SECURITY

55. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

56. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

57. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a) (1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

58. A Data Breach such as the one Defendant experienced is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule. *See* 45 C.F.R. 164.402 (Defining "Breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information.").

59. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to meet standards mandated by HIPAA regulations.

V. DEFENDANT'S BREACH

60. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

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

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

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

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures about PHI as necessary and appropriate for the members of its

workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption").

61. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing malignant computer code, and inadequately trained employees who opened files containing malicious software, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

62. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

63. Data Breaches such as the one experienced by Defendant's clients are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

64. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

65. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (possibly an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

[12] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited May 21, 2024) ("GAO Report").

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

66. Identity thieves use stolen personal information for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

67. Theft of Private Information is gravely serious. PII/PHI is a valuable property right.[14] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

68. Theft of PHI is also gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[15] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

69. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information

[13] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited August 19, 2024).
[14] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[15] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited May 21, 2024).

and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

70. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

71. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

72. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[16] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

73. Healthcare data, as one would expect, demands a much higher price on the black market. The National Association of Healthcare Access Management reports, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[17]

---

[16] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 21, 2024).

[17] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited August 30, 2024).

74. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[18]

75. In recent years, the healthcare industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

VI. PLAINTIFF'S EXPERIENCE

76. Plaintiff Sarah Sullivan is and at all times mentioned herein was an individual citizen of Montana, residing in the city of South Great Falls.

77. Plaintiff's minor child, M.S., received healthcare services from Defendant.

78. Plaintiff provided Defendant with her sensitive PII and the sensitive PII and PHI of M.S. as a condition of receiving Defendant's services.

79. After Plaintiff provided the Private Information, Defendant suffered a Data Breach.

80. Plaintiff received notice from Defendant that her child's Private Information was put at risk because of the Data Breach. Specifically, Defendant's notice states that M.S.'s "name and date of birth, medical diagnosis and treatment information, health insurance information, medical record number, and date of service" were exposed in the Data Breach.

81. Plaintiff reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard her Private Information from unauthorized users or disclosure, and would timely notify her of any data

[18] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for-everyone/ (last visited March 10, 2022).

security incidents related to the same. Plaintiff would not have provided her Private Information to Defendant had she known that Defendant would not take reasonable steps to safeguard it.

82. Plaintiff is very careful about sharing her sensitive PII and PHI and that of her family. She has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff also stores any documents containing her sensitive information in a safe and secure location or destroys the documents.

83. Because of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach and monitoring her financial statements and accounts.

84. Plaintiff has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

85. Plaintiff is especially alarmed by the amount of stolen or accessed PII and PHI listed in Defendant's notice. Despite Defendant providing that list, Plaintiff cannot be sure whether more PII or PHI was exfiltrated.

86. Plaintiff knows that cybercriminals often sell Private Information, and that her child's PII or PHI could be abused months or even years after a data breach.

87. Had Plaintiff been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her family's personal data.

VII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

88. To date, Defendant has done nothing to compensate Plaintiff and Class Members for the damages they sustained in the Data Breach.

89. Defendant's failure to compensate is wholly inadequate as it fails to make whole all victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and

it provides no compensation for its unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

90. Defendant's advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

91. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

92. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

93. Plaintiff was damaged in that her family's Private Information is in the hands of cybercriminals.

94. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

95. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

96. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

97. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

98. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

99. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

100. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

101. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably spent to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing “freezes” and “alerts” with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

102. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

103. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

104. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

VIII. CLASS ACTION ALLEGATIONS

105. This action is brought and may be properly maintained as a class action pursuant to M.C.A. § 25-20-23.

106. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

107. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised because of the August 24-28, 2024 Data Breach (the "Class").**

108. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

109. Plaintiffs reserve the right to amend or modify the class definition with greater specificity or division after having an opportunity to conduct discovery.

110. Numerosity. The Members of the Class are so numerous that joinder of all of them in a single proceeding is impracticable. The exact number of Class Members is unknown to Plaintiff now, but Defendant has reported to the U.S. Department of Human Services Office for Civil Rights that 18,003 individuals were affected by the Data Breach.

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant failed to provide notice of the Data Breach promptly; and

j. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

112. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

113. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

114. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

115. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy.

116. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

117. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

118. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

IX. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

119. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

120. Defendant required Plaintiff and Class Members to submit non-public personal information to obtain healthcare services.

121. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

122. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

123. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as common law. Defendant could have ensured that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

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

125. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to

protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all the healthcare information at issue constitutes "protected health information" within the meaning of HIPAA.

126. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

127. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

128. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to store Class Members' Private Information in an encrypted state;

f. Failing to detect timely that Class Members' Private Information had been compromised;

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

129. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

130. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

131. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

132. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

133. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

134. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

135. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

136. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

137. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and adhered to industry standards.

138. Plaintiff and Class Members paid money to Defendant or had money paid on their behalf with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

139. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

140. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

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

142. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

143. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

144. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

145. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

146. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

147. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

148. Under HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

149. Under HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

150. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide reasonable or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

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

153. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

by failing to meet its duties, it would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

155. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

156. Considering the confidential relationship between Plaintiffs and Defendant's physician-agents, Defendant owed a fiduciary duty to Plaintiffs and the Class to protect their private and sensitive Personal Information and keep them apprised of when that information becomes exposed or compromised in a timely manner.

157. Defendant breached that fiduciary duty by, inter alia, failing to comply with the guidelines outlined under HIPAA and the FTC Act for safeguarding and storing it. This failure resulted in the Data Breach that ultimately came to pass.

158. Defendant further breached its fiduciary duty by failing to dispose of Personal Information that was no longer required to render care, which unnecessarily exposed additional patients—including Plaintiff—to the Data Breach, and by failing to timely and accurately inform Plaintiffs and the Class of the Data Breach which materially impaired their mitigation efforts.

159. As a direct and proximate cause of Defendant's breaches of its fiduciary duty, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (a) the compromise, publication, theft, and /or unauthorized use of their Personal Information: (b) out- of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; (c) lost opportunity costs and lost wages associated with efforts expended and the

loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud: (d) the continued risk to their Personal Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect Personal Information in their possession; and (e) current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

160. Plaintiff and the Class seek compensatory damages for breach of fiduciary duty, which entails the amount of the difference between the price they paid for Defendants' services as promised and the diminished value of its health care services and the costs of future monitoring of their credit history for identity theft and fraud, and/or other damages, plus prejudgment interest, and costs.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself, her minor child M.S., and the Class described above, seeks the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and her counsel to represent the Class, and finding that Plaintiff is a proper representative of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;

e. For an Order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Any other relief that this Court may deem just and proper.

XI. JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: November 18, 2024

/s/ Teague Westrope
Attorney for Plaintiffs