IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF MISSISSIPPI SOUTHERN DIVISION

CASIE MEYER, on behalf of herself and all others similarly situated, **PLAINTIFF**

Plaintiff,

v. **CASE NO.:** 1:19-cv-700-HSO-JCG

MEMORIAL HOSPITAL AT GULFPORT FOUNDATION, INC. **DEFENDANT**

COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF (Collective Action Complaint)

Plaintiff, Casie Meyer ("Plaintiff"), individually, by and through her undersigned counsel, brings this class action lawsuit against Memorial Hospital at Gulfport ("MHG"), on behalf of herself and all others similarly situated, and alleges, based upon information and belief and the investigation of her counsel as follows:

INTRODUCTION

1. This is a putative class action lawsuit brought by current and former patients of MHG against Defendant for its failure to properly secure and safeguard the personally identifiable information of its patients, and for its failure to provide timely, accurate and adequate notice that such PII had been compromised.

2. On December 17, 2018, MHG discovered that one of its employees' email accounts had been compromised 11 days earlier, and as result, the personal health information ("PHI") and other personally identifiable information (collectively "PII") of approximately 30,000 MHG patients had been illegally exposed ("Data Breach").[1] The exposed PII included: names, dates of birth, health insurance

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on

information, and information about medical services received at the hospital. In several instances, the exposed PII also included Social Security numbers.

3. Although the Data Breach was discovered in December 2018, MHG waited nearly two months before publicly announcing that its patient PII had been exposed.

4. This Data Breach was preventable and a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patient PII.

5. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust security practices to safeguard patient PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

6. As a result of Defendant's failure to implement and follow basic security procedures, patient PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.

7. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, negligence per se, invasion of privacy, breach of implied contract, unjust enrichment, breach of fiduciary

---

their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (e.g. Social Security number, passport number, driver's license number, financial account number). Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, ("HIPAA"), protected health information ("PHI") is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

duty, and breach of confidence and seeks to compel Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices to safeguard patient PII that remains in its custody, in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

8. Plaintiff, Casie Meyer, is a resident of Bay St. Louis, Mississippi and a patient of MHG. On or about February 15, 2019, Ms. Meyer received notice from MHG that her PII, along with approximately 30,000 other patients, had been improperly exposed to unauthorized third parties.

9. After being notified of the Data Breach, Ms. Meyer contacted all three of the major credit bureaus. She also ordered a copy of her credit report which revealed that multiple attempts had been made by unauthorized parties to obtain loans and credit cards under her name. Ms. Meyer subsequently put a freeze on her credit.

10. Since the announcement of the Data Breach, Ms. Meyer continues to monitor her accounts in an effort to detect and prevent any misuses of her personal information.

11. Ms. Meyer has, and continues to, spend her valuable time to protect the integrity of her medical records, finances and credit – time which she would not have had to expend but for the Data Breach.

12. Plaintiff suffered actual injury from having her PII stolen as a result of the Data Breach including, but not limited to: (a) paying monies to MHG for its goods and services which she would not have had if MHG disclosed that it lacked computer systems and data security practices adequate to safeguard consumers' PII from theft; (b) damages to and diminution in the value of her PII—a form of intangible property that the Plaintiff entrusted to MHG as a condition for health services; (c) loss of her privacy; .(d) imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being exposed to criminals.

13. As a result of the Data Breach, Ms. Meyer will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and their attendant damages, for years to come.

14. Defendant Memorial Hospital at Gulfport is a not-for-profit medical complex in Gulfport, Mississippi, jointly owned by the City of Gulfport and Harrison County. It is one of the most comprehensive healthcare systems in the state, licensed for 303 beds, including a state-designated Level II Trauma Center, two outpatient surgery centers, satellite outpatient diagnostic and rehabilitation centers and more than 95 Memorial Physician Clinics. It is located at 4500 Thirteenth Street Gulfport, MS 39501.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are approximately 30,000 putative Class Members, at least some of whom have a different citizenship from MHG.

16. This Court has jurisdiction over the Defendant which operates in this District, and the data implicated in this Breach was generated and maintained in this District. MHG is also headquartered in this District.

17. Plaintiff was an MHG patient that received health services in this District where her PII was also maintained, and where the breach occurred which led her to sustain damage. Through its business operations, MHG intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. MHG is based in this District, maintains patient PII in the District and has caused harm to Plaintiff and Class Members residing in this District.

STATEMENT OF FACTS

A. The MHG Data Breach

19. On December 17, 2018, MHG learned that an unauthorized third party gained access to an employee's email account on December 6, 2018, through a successful phishing attack which resulted

in the exposure of the sensitive PII of approximately 30,000 MHG patients.[2] As a result of the attack, an unauthorized third party gained unfettered access to MHG patient PII over an 11 day period before the breach was discovered.

20. The exposed PII includes patients' names, dates of birth, health insurance information and/or information about medical care received at MHG and Social Security numbers.

21. On February 15, 2019, MHG issued the following announcement:

> GULFPORT, Miss. —Memorial Hospital at Gulfport ("MHG") announced that it is sending letters today to patients about a recent email phishing incident.
>
> On December 17, 2018, MHG learned that an unauthorized third party gained access to an employee's email account on December 6, 2018. MHG immediately took steps to secure the account and began an investigation, which determined that patient information was contained in the email account and may have included patients' names, dates of birth, health insurance information and/or information about medical care received at MHG. A limited number of Social Security numbers were also contained within the email account.
>
> Even though MHG has no indication that patient information has been misused, it began mailing letters to affected patients on February 15, 2019, and is offering complimentary credit monitoring and identity protection services to those patients whose Social Security numbers were included in the email account. MHG recommends that affected patients review statements they receive from their health care providers and health insurers. If they see charges or services not incurred or received, they should contact the insurer or provider immediately.
>
> * * *
>
> MHG takes the privacy and confidentiality of its patients' information very seriously and is enhancing its information security safeguards to help prevent an incident such as this from occurring in the future.[3]

B. Prevalence of Cyber Attacks and Particular Susceptibility of Hospital Systems

22. Cyber-attacks come in many forms. Phishing attacks are among the oldest, most common, and well known. In simple terms, phishing is a method of obtaining personal information using

---

[2] *HIPAA Journal*, February 18, 2019 ("Memorial Hospital at Gulfport, MS, is notifying approximately 30,000 patients that some of their protected health information has potentially been accessed by an unauthorized individual as a result of a phishing incident."). Available at https://www.hipaajournal.com/30000-patients-notified-of-phishing-incident-at-memorial-hospital-at-gulfport/.

[3] http://www.gulfportmemorial.com/news/memorial-notifies-patients-about-email-phishing-in-444

deceptive e-mails and websites. The goal is to trick an e-mail recipient into believing that the message is something they want or need from a legitimate or trustworthy source and to subsequently take and action such as clicking on a link or downloading an attachment. The fake link will typically mimic a familiar website and require the input of credentials. Once input, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware of.[4] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[5]

23. Phishing attacks are well known and understood by the cyber-protection community and are generally preventable with the implementation of a variety of proactive measures such as sandboxing inbound e-mail[6], inspecting and analyzing web traffic, penetration testing an organization to find weak spots[7], and employee education, among others.

24. Data breaches, including those perpetrated by phishing attacks, have become pervasive. In 2016, the number of U.S. data breaches surpassed 1,000, representing a record high and a forty percent increase from the previous year. [8] In 2017 a new record high of 1,579 breaches was reached representing

---

[4] https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.

[5] *All About Phishing*, Malwarebytes, https://www.malwarebytes.com/phishing/.

[6] An automated process whereby e-mails with attachments and links are segregated to an isolated test environment, a "sandbox," wherein a suspicious file or URL may be executed safely.

[7] *See*, https://searchsecurity.techtarget.com/definition/penetration-testing (The practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incident. The primary goal of a pen test is to identify weak spots in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether -- and how -- the organization would be subject to security disasters.)

[8] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at* https://www.idtheftcenter.org/surveys-studys/.

a 44.7% increase over 2016.[9] In 2018, the healthcare sector had the second largest number of breaches among all measured sectors and the highest rate of exposure per breach.[10]

25. Indeed, healthcare related data is among the most sensitive, and personally consequential when compromised. A report focusing on health-care breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000," and that the victims were routinely forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. [11] Almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all.[12]

26. Hospital data breaches in particular have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors" such as cybercriminals.[13]

27. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[14]

---

[9] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/2017-data-breaches/.

[10] Identity Theft Resource Center, 2018 End -of-Year Data Breach Report. Available at https://www.idtheftcenter.org/2018-data-breaches/.

[11] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[12] *Id.*

[13] https://www.himss.org/2019-himss-cybersecurity-survey.

[14] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

28. "Unfortunately, by the time medical identity theft is discovered, the damage has been done. Forty percent of consumers say that they found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that thieves incurred in their name. As a result, the consequences of medical identity theft are frequently severe, stressful and expensive to resolve." [15]

29. The consequences to affected consumers are further exacerbated when compromised PII includes Social Security numbers which make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect and may not be uncovered until the number has been used in a fraudulent transaction. Moreover, it is no easy task to change or cancel a stolen Social Security number. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

30. MHG knew the importance of safeguarding patient PII entrusted to it and of the foreseeable consequences if its data security systems were to be breached, including the significant costs that would be imposed on its patients as a result of a breach. Despite this knowledge, MHG failed to take adequate cyber-security measures to prevent the most basic of cyber intrusions – a phishing attack – from happening.

C. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

31. As a condition for obtaining health services, MHG requires that its patients provide highly sensitive personal information.

---

[15] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, Experian (April 2010). Available at https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[16] Naylor, B., *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

32. Defendant acquires, collects, stores, and maintains a massive amount of protected health related information and other personally identifiable information on its patients.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class Members' PII, MHG assumed legal and equitable duties to those individuals and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

34. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members, as current and former patients, relied on the Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Indeed, MHG maintains a Privacy Policy which specifically acknowledges its legal obligation to maintain the privacy of patient PII entrusted to it.

MEMORIAL HOSPITAL'S NOTICE OF PRIVACY REQUIREMENTS[17]

This Notice of Privacy Practices describes how medical information about you may be used and disclosed and how you may get access to this information. Please read it carefully.

Memorial Hospital ("Memorial") is dedicated to protecting your medical information. We are required by law to maintain the privacy of your medical information and to provide you with this Notice of our legal duties and privacy practices with respect to your medical information. Memorial is required by law to abide by the terms of this Notice.

You have the following rights with respect to your medical information:

- You have the right to receive notification in the event of a breach of your medical information.
- You have the right to receive an accounting of the disclosures of your medical information made by Memorial during the last six years or following April 14, 2003.

[17] http://www.gulfportmemorial.com/hipaa

Patient Bill of Rights[18]

- You have the right within the limits of the law, to expect personal privacy and confidentiality of information and records pertaining to your care.

D. MHG's Inadequate Cyber-Security Practices

36. "Email phishing remains the primary attack vector for nine out of 10 cyberattacks," and is well known in the cyber-security community.[19] Unquestionably MHG could have and should have employed numerous and effective countermeasures to prevent such an attack.

37. Generally, organizations can mount two primary defenses to phishing scams—employee education and technical security barriers.

38. Employee education is the process of adequately making employees aware of common phishing scams and implementing company-wide policies requiring unknown links or attachments to be sequestered and checked for authenticity. Employee education and established protocols for use of log-in credentials is the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access to personal information.

39. Organizations like MHG can also greatly reduce the flow of phishing e-mails by implementing certain security measures governing e-mail transmissions. For example, organizations can use a simple e-mail validation system that allows domain owners to publish a list of IP addresses that are authorized to send e-mail on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Organizations can also use e-mail authentication protocols that block e-mail streams which have not been properly authenticated.

40. Unfortunately, MHG failed to employ any of these defenses to the detriment of Plaintiff and tens of thousands of Class Members. As evidenced by the success of the phishing attack, it is clear that MHG failed to ensure that its employees were adequately trained on even the most basic of cybersecurity protocols, including:

---

[18] http://www.gulfportmemorial.com/patient-rights-responsibilities.

[19] https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks

a. How to detect phishing e-mails;

b. Effective password management and encryption protocols for internal and external e-mails;

c. Avoiding responding to e-mails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information; and

e. Implementing guidelines for maintaining sensitive data.

41. MHG's failures handed criminals patient PII and put Plaintiff and members of the Class at serious, immediate and ongoing risk for identity theft and fraud.

E. Defendant's Conduct Violates HIPAA and Industry Standard Practices

42. The Health Insurance Portability and Accountability Act ("HIPAA") enacts security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[20]

43. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is being properly maintained.[21]

44. Defendant's Breach resulted from a combination of insufficiencies that indicate that Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. MHG's security failures include, but are not limited to:

---

[20] HIPAA lists 18 type of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights and includes: names, addresses, any dates including dates of birth, social security numbers and medical record numbers among others.

[21] 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

a. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

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

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

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

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

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

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

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

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

F. Defendant Fails to Comply with FTC Guidelines

45. 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.[22]

46. 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.[23] The guidelines advise businesses to: 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.

47. The FTC 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.[24]

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited

---

[22] *Start With Security*, Federal Trade Commission, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[23] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[24] FTC, *Start With Security*, *supra* note 32.

by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. MHG's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

50. As with the FTC, the private sector has developed an array of best practices which should be deployed among responsible business seeking to protect PII from cyber-attack.

51. MHG was at all times fully aware of its obligation to protect patient PII because of its position as a trusted healthcare provider. MHG was also aware of the significant repercussions if it failed to do so because MHG collected sensitive data from its patients and knew that this data, if hacked, would result in injury to patients such as Plaintiff and Class Members.

G. Defendant Fails to Comply with Industry Standards

52. The healthcare industry continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number which continued to grow in 2018 (363 breaches).[25] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record. *Id.* As a result, both the government and private sector have developed industry best standards to address this growing problem.

53. The Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly

[25] 2018 End of Year Data Brach Report, Identity theft Resource Center (2018) https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf; https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry;

sensitive and valuable data." [26] DHHS highlights " several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture:" (a) proper encryption of PII; (b) educate and train healthcare employees on how to identify social engineering attacks; (c) review audit logs regularly in order to identify attempts by unauthorized individuals to gain access to PII PHI before they result in a data breach; (d) correct Configuration of Software and Network Devices.

54. The private sector has similarly identified the healthcare sector as being particularly vulnerable to cyber-attacks both because of the of value of the PII that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[27] It has also issued numerous best practices that can be employed to mitigate the threat of cyber-attacks.

55. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, however, MHG chose to ignore them. Sadly, only after the Breach MHG said it would "implement additional technical safeguards…. [p]rovid[e] additional staff training on identifying unauthorized access,… and secur[e] a specialized cybersecurity firm to further assist us in implementing system-wide policies and procedures to help prevent a similar incident from occurring in the future."[28] Each of these preventative measures have long been cornerstones in the list of industry best practices. They were known, or should have been known by MHG, whose failure to heed and properly implement them directly led to the Data Breach and the exposure of its patients' PII.

---

[26] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/

[27] See e.g., https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry; https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref.

[28] https://www.MHGcenter.com/MHG-counseling-center-notifies-individuals-of-possible-data-security-incident/

H. Plaintiff and Class Members Suffered Damages

56. The ramifications of Defendant's failure to keep Patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

57. Victims of medical identity theft can suffer significant financial consequences. "In some cases, they paid the healthcare provider, repaid the insurer for services obtained by the thief, or they engaged an identity service provider or legal counsel to help resolve the incident and prevent future fraud."[29]

58. Moreover, resolution of medical identity theft is time consuming to resolve. "Due to HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident." *Id.* Consequently, they remain at "risk for further theft or errors in [their] healthcare records that could jeopardize medical treatments and diagnosis." *Id.*

59. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

60. The Data Breach was a direct and proximate result of MHG's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

61. Defendant had the resources necessary to prevent the Breach, but neglected to adequately invest in data security measures, despite their obligations to protect patient PII

---

[29] *Fifth Annual Study on Medical Identity Theft*, Ponemon Institute LLC, (February 2015), available at https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65.

62. Had Defendant remedied the deficiencies in its data security systems and adopted security measures commonly used in the industry, they could have prevented the intrusions into their systems and, ultimately, the theft of PII.

63. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[30]

64. To date, MHG has offered patients only a 1-year membership in credit monitoring and identity protection services.[31] This is inadequate. As discussed above, victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft. Moreover, Defendant's offer does not address any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

65. Furthermore, Defendant's credit monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions "offering" the services to affected patients recommending they sign up for the services.

---

[30] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf.

[31] *Memorial Hospital at Gulfport Notice of Data Breach*, Office of the Vermont Attorney General …[W]e are offering you a complimentary one-year membership of Experian IdentityWorks Credit 3B." ("As an additional precaution, to reduce the risk of fraud or identity theft, we are offering a one-year membership in Experian's IdentityWorks at no cost to you."), https://ago.vermont.gov/blog/2019/06/14/memorial-hospital-at-gulfport-notice-of-data-breach-to-consumers/

66. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or 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 PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its 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 Plaintiff and Class Members.

67. In addition to a remedy for the economic harm, Plaintiff and the Class maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

68. Plaintiff seeks relief on behalf of herself and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons in the United States whose PII was compromised as a result of the Data Breach announced by MHG in December 2018 (the "Class").

69. Excluded from the Class are MHG and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

70. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

71. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

72. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. The Data Breach implicates at least 32,000 current and former MHG patients. MHG has physical and email addresses for Class members who therefore may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

73. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether MHG had a duty to protect patient PII;

b. Whether MHG knew or should have known of the susceptibility of its systems to a data breach;

c. Whether MHG's security measures to protect its systems were reasonable in light of best practices recommended by data security experts;

d. Whether MHG was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether MHG's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether MHG's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of MHG's failure to reasonably protect its systems and data network; and,

h. Whether Plaintiff and Class members are entitled to relief.

74. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is an MHG patient whose PII was exposed in the Data Breach. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class.

75. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class she seeks to represent; is committed to pursuing this matter against MHG to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

76. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against MHG, and thus, individual litigation to redress MHG's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class

action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

77. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

78. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether MHG failed to timely notify the public of the Data Breach;

b. Whether MHG owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether MHG's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

79. Finally, all members of the proposed Classes are readily ascertainable. MHG has access to patient names and addresses affected by the Data Breach. Using this information, Class members can be identified and ascertained for the purpose of providing notice.

FIRST CAUSE OF ACTION
NEGLIGENCE

80. Plaintiff restates and realleges paragraphs 1 through 79 above as if fully set forth herein.

81. As a condition of receiving services, Plaintiff and Class Members were obligated to provide MHG, through their respective insurance carriers, with their PII.

82. Plaintiff and the Class Members entrusted their PII to MHG with the understanding that MHG would safeguard their information.

83. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

84. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing the Defendant's security protocols to ensure that Plaintiff's and Class Members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of patient information.

85. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

86. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

87. Plaintiff and the Class Members had no ability to protect their PII that was in MHG's possession.

88. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

89. Defendant had a duty to have proper procedures in place to prevent the unauthorized dissemination Plaintiff and Class Members' PII.

90. Defendant has admitted that Plaintiff's and Class Members' PII was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

91. Defendant, through their actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff's and Class Members' PII while it was within the MHG's possession or control.

92. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

93. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII.

94. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class Members the existence, and scope of the Data Breach.

95. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

96. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

97. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting

the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE

98. Plaintiff restates and realleges Paragraphs 1 through 79 as if fully set forth herein.

99. Violation of statute which establishes a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence per se.

100. 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 MHG, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

101. MHG violated Section 5 of the FTC Act by failing to use reasonable measures to protect patient PII and not complying with applicable industry standards, as described in detail herein. MHG's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

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

103. The harm that occurred as a result of the Data 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 Plaintiff and the Class.

104. Based upon the conduct alleged herein, MHG's violation of Section 5 of the FTC Act constitutes negligence per se.

105. As a direct and proximate result of MHG's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not

limited to damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

106. Additionally, as a direct and proximate result of MHG's negligence per se, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Customer Data, which remain in MHG's possession and is subject to further unauthorized disclosures so long as MHG fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

THIRD CAUSE OF ACTION
INVASION OF PRIVACY

107. Plaintiff restates and realleges paragraphs 1 through 79 above as if fully set forth herein.

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

109. Defendant owed a duty to patients in their network, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

110. The unauthorized release of PII, especially the type related to personal health information, is highly offensive to a reasonable person.

111. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their use of MHG's services, but privately, with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

112. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

113. Defendant acted with a knowing state of mind when they permitted the Data Breach because they were with actual knowledge that their information security practices were inadequate and insufficient.

114. Because Defendant acted with this knowing state of mind, it had noticed and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

115. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

116. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

117. Plaintiff restates and realleges paragraphs 1 through 79 above as if fully set forth herein.

118. Plaintiff and Class Members were required to provide their PII, including names, addresses, dates of birth, social security numbers and various health related information to Defendant as a condition of their use of Defendant's services.

119. Plaintiff and Class Members paid money to Defendant in exchange for services, as well as Defendant's promises to protect their protected health information and other PII from unauthorized disclosure.

120. In their written privacy policies, MHG expressly promised Plaintiff and Class Members that they would only disclose protected health information and other PII under certain circumstances, none of which relate to the Data Breach.

121. MHG promised to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' protected health information and other PII would remain protected.

122. Implicit in the agreement between the Defendant's patients, including Plaintiff and Class Members, to provide protected health information and other PII, and Defendant's acceptance of such

protected health information and other PII, was Defendant's obligation to use the PII of their patients for business purposes only, take reasonable steps to secure and safeguard that protected health information and other PII, and not make unauthorized disclosures of the protected health information and other PII to unauthorized third parties.

123. Further, implicit in the agreement, Defendant was obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other PII.

124. Without such implied contracts, Plaintiff and Class Members would not have provided their protected health information and other PII to Defendant.

125. Defendant had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses.

126. Additionally, Defendant implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

127. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

128. Defendant breached the implied contracts with Plaintiff and Class Members by:

a. failing to reasonably safeguard and protect Plaintiff and Class Members' PII, which was compromised as a result of the Data Breach.

b. failing to comply with their promise to abide by HIPAA.

c. failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

d. failing to 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 in violation of 45 C.F.R. § 164.312(a)(1).

e. 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).

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

g. failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2).

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT

129. Plaintiff restates and realleges paragraphs 1 through 79 above as if fully set forth herein.

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

131. Defendant knew that Plaintiff and Class Members conferred a benefit on Defendant that Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

132. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

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

134. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

135. Defendant acquired the PII through inequitable means in thatit failed to disclose the inadequate security practices previously alleged.

136. If Plaintiff and Class Members knew that Defendant would not secure its PII using adequate security measures, they would not have engaged in transactions with Defendant.

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

138. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII of patients and in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

141. Plaintiff restates and realleges paragraphs 1 through 79 above as if fully set forth herein.

142. In light of the special relationship between Defendant and their Patients, whereby Defendant became a guardian of Plaintiff's and Class Members' highly sensitive, confidential PII. Defendant subsequently became a fiduciary created by its undertakings and guardianship of the PII, to act

primarily for the benefit of its patients to: 1) safeguard Plaintiff and Class Members' PII; 2) timely notify Plaintiff and Class Members' of a data breach or disclosure of their PII; and 3) maintain complete and accurate records of what and where Defendant's patients' information was and is stored.

143. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its patients' relationship, in particular to keep secure the PII of its patients.

144. Defendant breached its fiduciary duties to Plaintiff and Class Members by:

a. failing to diligently investigate the Data Breach to determine the number of Class Members affected in a reasonable and practicable period of time.

b. failing to encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' protected health information and other PII.

c. failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

d. failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

e. failing to 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 in violation of 45 C.F.R. § 164.312(a)(1).

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

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

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

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

j. failing to ensure compliance with the HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(94).

k. impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

l. failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

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

n. otherwise failing to safeguard Plaintiff's and Class Members' PII.

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

protect Patient PII in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

146. As a direct and proximate result of Defendant's breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SEVENTH CAUSE OF ACTION
BREACH OF CONFIDENCE

147. Plaintiff restates and realleges paragraphs 1 through 79 above as if fully set forth herein.

148. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' protected health information and other PII that Plaintiff and Class Members provided to Defendant.

149. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' protected health information and other PII would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

150. Plaintiff and Class Members provided their respective protected health information and PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the protected health information and other PII to be disseminated to any unauthorized parties.

151. Plaintiff and Class Members also provided their respective protected health information and PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that protected health information and other PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

152. Defendant voluntarily received in confidence Plaintiff's and Class Members' protected health information and other PII with the understanding that protected health information and other PII would not be disclosed or disseminated to the public or any unauthorized third parties.

153. Due to Defendant's failure to prevent, detect, avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Members' protected health information and other PII, Plaintiff's and Class Members' protected health information and PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

154. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

155. But for Defendant's disclosure of Plaintiff's and Class Members' protected health information and other PII in violation of the parties' understanding of confidence, their protected health information and other PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected health information and other PII, as well as the resulting damages.

156. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' protected health information and other PII. Defendant knew their computer systems and technologies for accepting and securing Plaintiff's and Class Members' protected health information and other PII had numerous security vulnerabilities because Defendant failed to observe even basic security practices necessary to prevent fraudulent provider accounts from being created.

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

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

158. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

a. An Order certifying this case as a class action;

b. An Order appointing Plaintiff as the class representative;

c. An Order appointing undersigned counsel as class counsel;

d. A mandatory injunction directing the Defendant to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

e. An award of damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

h. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial as to all issues triable by a jury.

Dated: October 11, 2019

Respectfully Submitted,
CASIE MEYER, PLAINTIFF

/s/ William A. Graves

WILLIAM A. GRAVES, MS Bar No. 105679
Morgan & Morgan, PLLC
4450 Old Canton Road, Ste. 200
Jackson, MS 39211
Tel: 601-603-1659
Email: wgraves@forthepeople.com

Jean Sutton Martin (*Pro Hac Vice to be submitted)*
jeanmartin@forthepeople.com
Ryan McGee (*Pro Hac Vice to be submitted)*
rmcgee@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908
Facsimile: (813) 223-5402
Counsel for Plaintiffs

JS 44 (Rev. 09/19)

CIVIL COVER SHEET

1:19-cv-700-HSO-JCG

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

CASIE MEYER, on behalf of herself and all others similarly situated,

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

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

DEFENDANTS

MEMORIAL HOSPITAL AT GULFPORT FOUNDATION, INC,

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

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

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Negligence, Negligence per se, Invasion of Privacy, Breach of Implied Contract, Unjust Enrichment, et al.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 10/11/2019

SIGNATURE OF ATTORNEY OF RECORD /s/ William A. Graves

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $400.00 APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

#0538-4112524

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Class Action: Memorial Hospital Waited Nearly Two Months to Disclose Data Breach Affecting 30K Patients