UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

KATHLEEN TUCKER, SHARON CHADDOCK, GERALD DAVIS, DONNA ACREE, CINDY BEAVER, on behalf of herself and all others similarly situated, Plaintiffs v. **MARIETTA AREA HEALTH CARE, INC. D/B/A MEMORIAL HEALTH SYSTEM,** Defendant.	Case No. 2:22-cv-00184-SDM-EPD **Judge Sarah D. Morrison** **Magistrate Judge Elizabeth P. Deavers** JURY TRIAL DEMANDED

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Kathleen Tucker, Sharon Chaddock, Gerald Davis, Donna Acree, and Cindy Beaver ("Plaintiffs"), individually and on behalf of themselves and all others similarly situated, bring this Consolidated Amended Class Action Complaint against Defendant Marietta Area Health Care, Inc. dba Memorial Health System (hereinafter known as "MHS" or "Defendant"). Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record:

NATURE OF THE ACTION

1. Defendant MHS is a regional medical services business that provides a wide range of medical services including, but not limited to, emergency, surgical, rehabilitation, oncology, pediatric, and psychological care in both inpatient and outpatient settings. The network has business locations and operates throughout southeastern Ohio and northwestern West Virginia.

2. This class action arises out of the recent targeted cyberattack against Defendant's

computer network. During the course of the attack, the criminal third party gained access to Defendant MHS's computer systems and likely acquired the highly sensitive personal information belonging to approximately 216,478 current and former patients (the "Data Breach"). The type of information compromised in the Data Breach included the personally identifiable information ("PII") of Defendant's patients, such as the names, dates of birth, patient account numbers, medical record numbers, and Social Security numbers, as well as protected health information ("PHI"), including medical treatment information. ("PII" and "PHI" will be collectively referred to as "Sensitive Information")

3. The full extent of the types of Sensitive Information, the scope of the breach, and the root cause of the Data Breach is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of the litigation. Upon information and belief, the Data Breach resulted in additional types of Sensitive Information that Defendant routinely collected and maintained on the network that was compromised but has not been disclosed with specificity in the current notice discussed herein—e.g., health insurance information, diagnostic results, genetic testing results, etc.

4. Notwithstanding, Defendant has admitted that an "authorized actor accessed certain systems within [its] network" and that "sensitive information was present in the affected systems." Defendant further admitted that it was "possible that this information could have been…acquired by an unauthorized actor."[1]

5. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Sensitive Information that it collected and maintained.

[1] https://mhsystem.org/assets/documents/DataNotice.pdf (last visited April 29, 2022) (attached as **Exhibit 1**).

6. Defendant MHS is responsible for allowing this Data Breach because of multiple acts of negligence and recklessness, including but not limited to its: failure to design, implement, and maintain reasonable data security systems and safeguards; failure to exercise reasonable care in the hiring, supervision, and training of its employees and agents and vendors; failure to comply with industry-standard data security practices; and failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action.

7. Despite its role in managing so much Sensitive Information, Defendant failed to take basic security measures such as encrypting its data. Moreover, Defendant failed to recognize and detect that unauthorized third parties had accessed its network and, upon information and belief, further failed to recognize that substantial amounts of data had been compromised, and more likely than not, acquired, exfiltrated and stolen. Had Defendant not committed the acts of negligence and recklessness described herein, it would have discovered the Data Breach sooner – and/or prevented the invasion and theft altogether.

8. Defendant owed numerous statutory, regulatory, contractual, and common law duties to Plaintiffs and Class Members to protect and keep their Sensitive Information confidential, safe, secure, and protected from unauthorized disclosure, access, and unconsented acquisition and exfiltration, including duties found within its own privacy policy, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Federal Trade Commission Act, 15 U.S.C. § 45. ("FTCA").

9. Moreover, by obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class Members' Sensitive Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members'

Sensitive Information from unauthorized access, disclosure, and theft due to criminal hacking activity.

10. As patients of Defendant, Plaintiffs and Class Members were required to provide their Sensitive Information to Defendant as a condition to receive medical services.

11. In acquiring and maintaining Plaintiffs' and Class Members' Sensitive Information, Defendant expressly and impliedly promised to safeguard Plaintiffs' and Class Members' Sensitive Information.

12. Plaintiffs and Class Members reasonably relied upon Defendant to maintain the security and privacy of the Sensitive Information entrusted to it. Plaintiffs and Class Members further relied on Defendant to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

13. Plaintiffs and Class Members reasonably expected and understood that Defendant would ensure that it would comply with its numerous duties, promises, and obligations to keep Plaintiffs' and Class Members' Sensitive Information secure and safe from unauthorized access. Defendant, however, breached its duties, promises, and obligations, and Defendant's failures increased the risk that Plaintiffs' and Class Members' Sensitive Information would be compromised in the event of a likely cyberattack.

14. Plaintiffs and Class Members would not have paid the amounts they paid for medical services, had they known their sensitive information would be maintained using inadequate data security systems.

15. In this era of frequent data security attacks and data breaches, particularly in the healthcare industry, Defendant's failures leading to the Data Breach are particularly egregious,

as this Data Breach was highly foreseeable.

16. Upon information and belief, as a result of Defendant's failures to protect the Sensitive Information of Plaintiffs and Class Members, their Sensitive Information was disclosed, accessed, acquired, downloaded, and/or exfiltrated by malicious cyber criminals, who targeted that information through their wrongdoing. As a direct and proximate result, Plaintiffs and Class Members are now at a significant present and future risk of identity theft, financial fraud, health care identity fraud, and/or other identity-theft or fraud, imminently and for years to come.

17. In the months and years following the Data Breach, Plaintiffs and the other Class Members will experience numerous types of harms as a result of Defendant's ineffective and inadequate data security measures. Some of these harms will likely include fraudulent charges on financial accounts, opening fraudulent financial accounts, acquiring medical procedures and prescriptions ordered in patients' names, and targeted advertising without patient consent.

18. Plaintiffs and Class Members have also now lost the economic value of their Sensitive Information. Indeed, there is both a healthy black market and a legitimate market for that Sensitive Information. Just as Plaintiffs' and Class Members' Sensitive Information were stolen, *inter alia*, because of its inherent value in the black market, the inherent value of Plaintiffs' and the Class Members' Sensitive Information in the legitimate market is now significantly and materially decreased.

19. Plaintiffs and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their Sensitive Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the

emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) the diminution in value of their personal data; (h) the loss of value of the bargain for paying for services that required entrusting their Sensitive Information to Defendant with the mutual understanding that Defendant would safeguard the Sensitive Information against improper disclosure, misuse, and theft; and (h) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

20. Plaintiffs seek to remedy these harms, and to prevent their future occurrence, on behalf of themselves and all similarly situated persons whose Sensitive Information were compromised as a result of the Data Breach.

21. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for Negligence (Count I), Negligence Per Se (Count II), Breach of Express Contract (Count III), Breach of Implied Contract (Count IV), Breach of Fiduciary Duty (Count V), and Unjust Enrichment (Count VI). Plaintiffs also seek Declaratory Judgment and Injunctive Relief (Count VII).

PARTIES

Plaintiff Kathleen Tucker

22. Plaintiff Kathleen Tucker is a resident and citizen of the State of West Virginia and intends to remain domiciled in and a citizen of the State of West Virginia.

23. Plaintiff Tucker received a letter dated January 10, 2022 from Defendant

concerning the Data Breach. The letter stated that unauthorized actors accessed MHS's network containing her name, Social Security number, medical/treatment information, and health insurance information.

Plaintiff Sharon Chaddock

24. Plaintiff Sharon Chaddock is a resident and citizen of the State of West Virginia and intends to remain domiciled in and a citizen of the State of West Virginia.

25. Plaintiff Chaddock received a letter dated January 10, 2022 from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed MHS's network containing her name, Social Security number, medical/treatment information, and health insurance information.

Plaintiff Gerald Davis

26. Plaintiff Gerald Davis is a resident and citizen of the State of West Virginia and intends to remain domiciled in and a citizen of the State of West Virginia.

27. Plaintiff Davis received a letter dated January 10, 2022 from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed MHS's network containing his name, Social Security number, medical/treatment information, and health insurance information.

Plaintiff Donna Acree

28. Plaintiff Donna Acree is a resident and citizen of the State of South Carolina and intends to remain domiciled in and a citizen of the State of South Carolina.

29. Plaintiff Acree received a letter dated January 10, 2022 from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed MHS's network containing her name, Social Security number, medical/treatment information, and health insurance

information.

Plaintiff Cindy Beaver

30. Plaintiff Cindy Beaver is a resident and citizen of the State of Ohio and intends to remain domiciled in and a citizen of the State of Ohio.

31. Plaintiff Beaver received a letter dated January 10, 2022 from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed MHS's network containing her name, Social Security number, medical/treatment information, and health insurance information.

Defendant MHS

32. Defendant MHS is a domestic corporation organized under the laws of the State of Ohio with its principal place of business located at 401 Matthew Street, Marietta, Ohio 45750.

JURISDICTION AND VENUE

33. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2) ("CAFA"). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and several named Plaintiffs and Members of the proposed Class are citizens of West Virginia, and Defendant is a citizen of Ohio. Accordingly, minimal diversity under CAFA exists.

34. The Southern District of Ohio has general personal jurisdiction over Defendant because Defendant is organized under the laws of Ohio and is headquartered in this District.

35. Venue is proper in this Court pursuant to 28 U.S.C. §1391(b)(1) and (2) because: (1) Defendant resides in this judicial district, and (2) a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Background

36. MHS is a sophisticated health system comprised of a network of hospitals, emergency departments and outpatient service sites including, but not limited to, Marietta Memorial Hospital, Sistersville General Hospital, Selby General Hospital, Physicians Care Express; Marietta Health Care Physicians, Inc., Memorial Health Foundation, Marietta Occupational Health Partners, and Marietta Home Health Services & Hospice.[2]

37. MHS employs over 2,700 employees, including 325 providers representing 64 clinics. The system in total works with over 500 physicians representing over 40 specialties.[3]

38. Upon information and belief, in the ordinary course of rendering healthcare care services, MHS requires patients (including Plaintiffs and Class members) to provide sensitive, personal, and private information such as:

- Name, address, phone number, and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Health insurance information;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Photo identification; and
- Other information that may be deemed necessary to provide care.

39. As a condition of receiving and purchasing healthcare services from Defendant, Plaintiffs did in fact provide their Sensitive Information to Defendant, as a prerequisite to

[2] https://www.mhsystem.org/ourlocations (last visited April 26, 2022).
[3] *Id.*

receiving treatment and care from Defendant.

40. Additionally, MHS received Sensitive Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends, and/or family Members.

41. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Sensitive Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Sensitive Information from unauthorized disclosure. Plaintiffs and Class Members relied on Defendant to keep their Sensitive Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

Defendant's Privacy Policy

42. Upon information and belief, MHS provides each of its patients (including Plaintiffs) with a HIPAA compliant notice titled "Notice of Privacy Practices" (the "Privacy Notice") that explains how it handles patients' sensitive and confidential information.[4] The Privacy Notice is posted on Defendant's website[5] and, upon information and belief, provided to each patient (including Plaintiffs) prior to receiving treatment or services and upon request.

43. The Privacy Notice expressly promises that the Sensitive Information at issue in this Data Breach would only be disclosed for specific medical and business purposes: (1) for medical treatment; (2) for payment; (3) health care operations (risk assessment or quality care improvement); (4) appointments; (5) fund raising; and (6) hospital directory. The Privacy Notice

[4] *See* https://mhsystem.org/noticeofprivacypractice (last visitedApril 29, 2022) (attached as **Exhibit 2**).
[5] *Id.*

also allows for disclosure to comply with public health issues (e.g, child abuse), organ donation, or worker's compensation. The Privacy Notice then promises its patients that written authorization will be obtained prior to release in "a manner not described in this notice."[6]

44. The Privacy Notice also provides a specific promise that patients may invoke remedial rights in the event of an unauthorized disclosure—that is, Patients have the right to (1) request an accounting of all disclosures where the disclosure was not made for treatment, payment, operations, etc.; and (2) receive written notification of any inappropriate release or use of the protected health information.[7]

45. Finally, because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, MHS (a) acknowledges that it is "required to…maintain the privacy of protected health information;" (b) promises to inform patients of its legal duties and comply with laws protecting patients' PHI; (c) promises only to use and release patients' health information for approved reasons; (d) promises that it will "notify [patients] of certain breaches or inappropriate use or release of [their] information;" and (e) promises to adhere to the terms outlined in the Privacy Notice.[8]

46. As described herein, Defendant breached each of these expressed promises when it failed to safeguard the Sensitive Information and failed to institute a timely and fully informative Date Breach Notice program.

The Data Breach Was Foreseeable

47. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the

[6] *Id.*
[7] *Id.*
[8] *Id.*

date of the breach.

48. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[9] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[10] These 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only approximately 10 million sensitive records (9,700,238) in 2020.[11]

49. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic medical records and data systems would be targeted by cybercriminals.

50. Indeed, cyberattacks 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. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[12] Many

---

[9] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[10] *Id*.
[11] *Id*.
[12] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi- secret-service-warn-of-targeted-ransomware (last visited Jan. 25, 2022).

ransomware variants that have been used recently have expanded to include data exfiltration.[13]

51. According to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[14]

52. 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.

Data Breaches Are Known and Recognized to Cause Financial Harm to Patients

53. 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."[15]

54. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII and PHI is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, taking over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a

---

[13] *See* https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/ (last visited April 27, 2022).

[14] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited April 29, 2022).

[15] *See* U.S. Gov. Accounting Office, GAO-07-737, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 25, 2022).

person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

55. 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 (an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[16]

56. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture. Identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

57. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[17] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social

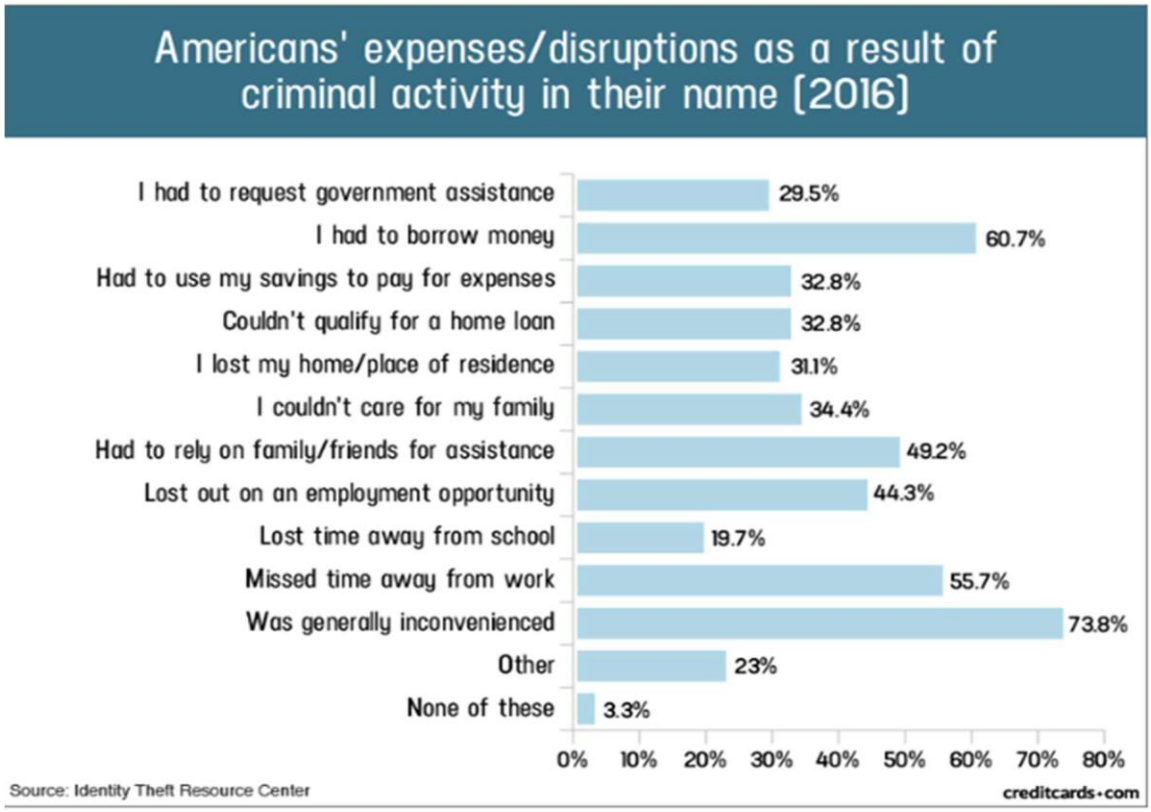
[16] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 25, 2022).
[17] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 25, 2022).

Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[18] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

58. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. 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."

59. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[19]

[18] *Id*. at 4.
[19] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Jan. 25, 2022).



60. Medical information is especially valuable to identity thieves.

61. 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.[20] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[21] Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

62. 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

[20] *See* Omri Toppol, Email Security: How You Are Doing It Wrong & Paying Too Much, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last visited Jan. 25, 2022).

[21] Lisa Vaas, Cyberattacks Paralyze, and Sometimes Crush, Hospitals, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals// (last visited Jan. 25, 2022).

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."[22]

63. Data breach incidents cause patients issues with receiving care that rise above the level of mere inconvenience. The issues that patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling their medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment; and

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. inability to access their medical records.[23]

64. This leads to a deterioration in the quality of overall care patients receive at facilities affected by data breaches. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[24] Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration

[22] *See* Federal Trade Commission, What to Know About Medical Identity Theft, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft identity-theft (last visited Jan. 25, 2022).

[23] *See, e.g.*, Vaas, Cyberattacks, supra, n. 21; Jessica David, Data Breaches Will Cost Healthcare $4B in 2019. Threats Outpace Tech, Health IT Security (Nov. 5, 2019), https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech (last visited Jan. 25, 2022).

[24] *See* Nsikan Akpan, Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart- attacks (last visited Jan. 25, 2022).

in timeliness and patient outcomes, generally.[25]

65. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and 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.

66. For all, there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Sensitive Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding 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.

67. Criminals often trade the information on the "cyber black-market" for years. One article referenced use of data from a breach that was used to commit fraud four years after the breach. [26]

68. Theft of Sensitive Information results in the loss of a valuable property right.[27]

---

[25] *See* Sung J. Choi et al., Cyberattack Remediation Efforts and Their Implications for Hospital Quality, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Jan. 25, 2022).

[26] *See* https://www.cybertalk.org/2018/06/20/4-years-later-data-opm-data-breach-used-commit-fraud/ (last visited April 27, 2022).

[27] *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).

69. Sensitive Information, as one would expect, demands a high price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

70. The value of Sensitive Information is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Sensitive Information can sell for as much as $363 per record according to the Infosec Institute.[28]

Federal Trade Commission Standards

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices to help avoid the known damaging consequences of a data breach. According to the FTC, the need for data security should be factored into all business decision- making.

72. 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.[29] The guidelines also recommend that businesses use an intrusion detection

[28] *See* Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 25, 2022).

[29] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 29, 2022).

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.[30]

73. 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.

74. 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 further clarify the measures businesses must take to meet their data security obligations.

75. 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.").

HIPAA Standards

76. HIPAA also requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

[30] *Id.*

77. Covered entities (including Defendant) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

78. 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 PII 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).

79. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. *See* 45 C.F.R.164.308(a)(6).[31]

80. Defendant is also subject to industry standards. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information that they collect and maintain.

[31] FACT SHEET: Ransomware and HIPAA, U.S. Department of Health & Human Services Office for Civil Rights (2016). Available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4 (last visited April 27, 2022).

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

82. 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; and training staff regarding critical points.

THE MHS CYBERATTACK

83. On August 14, 2021, MHS identified the presence of malware on the Marietta servers that was impacting all three MHS hospitals in Ohio and West Virginia.

84. The Data Breach resulted in a ransomware group encrypting the Hospital System and shutting down the IT systems.[32]

85. Emergency protocols were implemented that forced the medical staff off-line and to work with paper charts until the system could be restored thereby placing patients at risk for medical errors. With no access to radiology or electronic charts, MHS decided to divert emergency patients to other hospitals. Moreover, all urgent surgical appointments and radiology examinations were cancelled.[33]

[32] https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/ (last visited April 27, 2022).
[33] https://www.hipaajournal.com/cyberattack-forces-memorial-health-system-to-divert-patients-to-alternate-hospitals/ (last visited Jan. 19, 2022).

86. It was reported that Hive ransomware ("Hive"), a known data security threat group, was responsible for the attack. Hive has a common course of conduct of exfiltrating and stealing data once the data is accessed. Hive maintains a leak site on the Dark Web that is used to pressure victims into paying the ransom once it obtains the sensitive information.[34] "By exfiltrating information, the attackers have more leverage to force the victim to pay the ransom in exchange for the promise to not share or leak the stolen data and to provide a decryption tool."[35]

87. Upon information and belief, Plaintiffs' and Class Members' information was exfiltrated and stolen in the attack. Indeed, Bleeping Computer reported that evidence has been obtained that suggest databases containing the Sensitive Information were stolen in the attack.[36]

88. MHS "worked with a national cybersecurity experts to resolve the impact of a cyberattack in the early morning hours of August 15, 2021."[37]

89. Through the investigation, MHS determined that from July 10, 2021 through August 15, 2021, an unauthorized actor had "accessed certain systems within their network."[38]

90. Furthermore, the investigation determined that the accessed systems contained sensitive information and that was accessible, unprotected and vulnerable for acquisition and/or exfiltration by the unauthorized actor.[39]

91. The type of Sensitive Information that was accessed and acquired by the unauthorized actor included includes names, dates of birth, medical record numbers, patient account numbers, Social Security numbers, and medical and treatment information.[40]

---

[34] *Id*.
[35] https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/ (last visited Jan. 19, 2022).
[36] *Id*.
[37] *Id*.
[38] **Exhibit 1**.
[39] *Id*.
[40] *Id*.

92. As a result of the Data Breach, MHS was required to follow "a deliberate, systematic approach to bring systems back online securely and in a manner that prioritizes [MHS's] ability to provide patient care."[41] In addition, the investigation revealed that approximately 216,478 individuals were victims of the Data Breach.[42]

93. While MHS stated in the "Notice of Data Security Incident" letters received by Plaintiffs and Class Members ("Notice of Data Breach letter") that on August 15, 2021 it "detected the presence of malware on certain servers," MHS did not begin notifying victims until January 10, 2022 – approximately five months after discovering the Data Breach.

94. What is more, in the notices that MHS belatedly provided, MHS openly admitted that its systems containing Plaintiffs' and Class Members Sensitive Information were accessed, and further indicates that Plaintiffs' and Class Members' Sensitive Information was likely "acquired" by the cyberthieves who perpetrated the Data Breach.[43] This means that not only did the cybercriminals view and access the Sensitive Information without authorization, but they also removed Plaintiffs' and Class Members' Sensitive Information from MHS's network.

95. Upon information and belief, Plaintiffs' Sensitive Information was both stolen in the Data Breach (a fact indicated by Defendant in its Notice of Data Breach letter where Defendant states that the cybercriminals "acquired" the data) and is still in the hands of the hackers[44]. Plaintiffs further believe their Sensitive Information was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals who perpetrate cyberattacks of the type that occurred here.

---

[41] *Id*.
[42] https://apps.web.maine.gov/online/aeviewer/ME/40/e7861ebb-6f43-4fe7-9619-25762e3be35d.shtml (last visited April 27, 2022).
[43] Exhibit 1.
[44] *Id.*

96. While at one time the prime motive of a ransomware attack was simply to encrypt a user's data and hold it for ransom, ransomware attacks are now primarily the last phase of a multi-pronged cyberattack that is targeted to access and steal confidential data, like the Sensitive Information that was targeted here.

97. Indeed, a recent analysis shows that data exfiltration occurs in 70% of all ransomware attacks.[45] This means that third parties not only encrypt Sensitive Information to demand a ransom, but also have stolen and keep the PII after the ransom is paid.

DEFENDANT'S NEGLIGENT ACTS AND BREACH

98. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and 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;

b. Failing to adequately protect patients' Sensitive Information;

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

d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security

[45] Jessica Davis, *70% Ransomware Attacks Cause Data Exfiltration; Phishing Top Entry Point*, HealthITSecurity (Feb. 3, 2021), https://healthitsecurity.com/news/70-ransomware-attacks-cause-data-exfiltration-phishing-top-entry-point (last visited Feb. 11, 2022).

software protections to adequately protect against a blunt force intrusion;

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

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

h. 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);

i. 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);

j. 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);

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

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

m. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its

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

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it 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 CFR 164.304 definition of encryption).

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

p. Failing to adhere to industry standards for cybersecurity.

99. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI is a violation of FTC Guidelines and constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. A Data Breach such as the one Defendant experienced is also 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. 164.40.

100. The security failures listed above are also a violation of basic industry standards. 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.

PLAINTIFFS AND CLASS MEMBERS HAVE SUFFERED FORESEEABLE INJURY

101. To date, Defendant has failed to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has merely offered Plaintiffs and Class Members fraud and identity monitoring services for up to twelve (12) months, but this is insufficient for damage that will last years, and does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. What is more, Defendant places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

102. Plaintiffs and Class Members have been damaged by the compromise of their Sensitive Information in the Data Breach. Plaintiffs and Class Members suffered actual injury from having their Sensitive Information compromised as a result of the Data Breach including, but not limited to (a) 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; (b) emotional distress as a result of the release to cybercriminals of their Sensitive Information; (c) the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach; (d) damage to and diminution in the value of their Sensitive Information, a form of property that MHS obtained from Plaintiffs and Class Members; (e) violation of their privacy rights; and (f) imminent and impending injury arising from the increased risk of identity theft and fraud.

103. Plaintiffs and Class Members have and will incur damages as a direct result of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

f. Closely reviewing and monitoring Social Security number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

104. Plaintiffs and Class Members were also injured by and suffered benefit-of-the-bargain damages from this Data Breach. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiffs' and Class Members' Sensitive Information. Thus, Plaintiffs and Class Members did not get what they paid for and agreed to.

105. Moreover, Plaintiffs have not received full and adequate accounting and notification of the types of information that was accessed and likely exfiltrated.

106. Finally, Plaintiffs and Class Members have an interest in ensuring that their Sensitive Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but

not limited to, making sure that the storage of data or documents containing Sensitive Information is not accessible online and that access to such data is password protected.

Plaintiff Kathleen Tucker

107. Plaintiff Tucker used MHS's services over the past seven years, for various care and treatment. To receive services at MHS, Plaintiff Tucker was required to provide her Sensitive Information directly to Defendant's database, which is maintained by Defendant.

108. Plaintiff Tucker greatly values her privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her Sensitive Information.

109. Recognizing the substantial risk Plaintiff Tucker faces from the Data Breach, Defendant provided Plaintiff Tucker a one-year subscription to a credit monitoring service. However, Plaintiff Tucker did not opt to use these services due to her mistrust of the Defendant; in addition, Plaintiff Tucker uses Credit Karma for credit monitoring services.

110. Since learning of the Data Breach, Plaintiff Tucker has spent significant time reviewing her financial accounts, checking Credit Karma, ordering a new credit card and resetting her automatic payments with all of her providers.

111. Plaintiff Tucker has experienced actual fraud as a result of the data breach in the form of two unauthorized charges on her Discover credit card. Upon information and belief, this card was the same card she provided to Defendant to pay for medical services. Plaintiff Tucker was able to get reimbursement from her bank for the charges. As a result of these fraudulent charges, Plaintiff Tucker closed this credit card and ordered a new credit card. Plaintiff Tucker subsequently had to spend a significant amount of time updating her automatic payments with all of her providers to her new credit card.

112. Plaintiff Tucker has experienced an increase in spam phone calls and text messages as a result of this data breach since approximately September 2021. Plaintiff Tucker has been receiving spam phone calls and text messages that are both medically related and general spam calls.

113. The Data Breach has caused Plaintiff Tucker to suffer significant anxiety, fear, and uneasiness due to concerns for future identity theft.

114. Plaintiff Tucker plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as, monitoring her credit and identity, and checking her financial accounts more frequently.

Plaintiff Sharon Chaddock

115. Plaintiff Chaddock used MHS's services over the past five to seven years, mostly for emergency room services. To receive services at MHS, Plaintiff Chaddock was required to provide her Sensitive Information directly to Defendant's database, which is maintained by Defendant.

116. Plaintiff Chaddock greatly values her privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her Sensitive Information.

117. Recognizing the substantial risk Plaintiff Chaddock faces from the Data Breach, Defendant provided Plaintiff Chaddock a one-year subscription to a credit monitoring service. However, Plaintiff Chaddock did not opt to use these services, rather Plaintiff Chaddock uses credit monitoring services offered through Capital One.

118. Since learning of the Data Breach, Plaintiff Chaddock has spent significant time reviewing her financial accounts, researching the data breach, and has also spent time speaking

with her bank regarding her concerns about the Data Breach.

119. Capital One has notified Plaintiff Chaddock twice that her email was found on the Dark Web. As a result of these notifications, Plaintiff Chaddock went online and changed her password twice.

120. The Data Breach has caused Plaintiff Chaddock to suffer significant anxiety, anger, and nervousness due to concerns for future identity theft.

121. Plaintiff Chaddock plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as, monitoring her credit and identity, and checking her financial accounts more frequently.

Plaintiff Gerald Davis

122. Plaintiff Davis used MHS's services over the past seven years for various care and treatment. To receive services at MHS, Plaintiff Davis was required to provide his Sensitive Information directly to Defendant's database, which is maintained by Defendant.

123. Plaintiff Davis greatly values his privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of his Sensitive Information.

124. Recognizing the substantial risk Plaintiff Davis faces from the Data Breach, Defendant provided Plaintiff Davis a one-year subscription to a credit monitoring service. Plaintiff Davis opted to use this service, which required him to spend time signing up for the service.

125. Since learning of the Data Breach, Plaintiff Davis has spent significant time reviewing his financial accounts, researching the data breach, and has also spent time speaking with his bank regarding suspicious charges he has noticed on his accounts.

126. Plaintiff Davis has spent a significant amount of time contacting all three credit

bureaus to implement a credit freeze on his account. He was not charged for this service, but did spend time on the phone with each credit bureau. Moreover, the credit freeze will cause Mr. Davis additional inconvenience and lost time because he will be required to take time consuming steps to remove the credit freeze when applying for new credit.

127. Plaintiff Davis was notified that hackers may have his medical history. Since January 2022, Plaintiff Davis has received 10-15 phone calls a day from scammers claiming to be Medicare. These individuals have his Medicare Number, the last four digits of his Social Security number, and extensive knowledge of his family medical history. Plaintiff Davis has also gotten an increase in spam calls related to obtaining additional care, tests, and offers on medical devices.

128. Plaintiff Davis has experienced actual fraud in the form of fraudulent charges on his PayPal account. Plaintiff Davis noticed numerous fraudulent charges on his PayPal account starting in October 2021. Plaintiff Davis was able to freeze his account while he spent time fighting these charges. He was ultimately able to get reimbursement for only half of the charges, totaling approximately $80.

129. The Data Breach has caused Plaintiff Davis to suffer significant nuisance and annoyance.

130. Plaintiff Davis plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as, monitoring his credit and identity, and checking his financial accounts more frequently.

Plaintiff Donna Acree

131. Plaintiff Acree used MHS's services over the past nine years, for various care and treatment. To receive services at MHS, Plaintiff Acree was required to provide her Sensitive Information directly to Defendant's database, which is maintained by Defendant.

132. Plaintiff Acree greatly values her privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her Sensitive Information.

133. Recognizing the substantial risk Plaintiff Acree faces from the Data Breach, Defendant provided Plaintiff Acree a one-year subscription to a credit monitoring service. However, Plaintiff Acree did not opt to use these services, rather Plaintiff Acree checks her credit report herself about once a month.

134. Since learning of the Data Breach, Plaintiff Acree has spent significant time reviewing her financial accounts, researching the data breach, researching how to protect herself in the future, and has also spent time speaking with Venmo regarding fraudulent charges on her Venmo Account.

135. Plaintiff Acree has experienced actual fraud in the form of four unauthorized charges on her Venmo Credit Card. Plaintiff has spent time on the phone with Venmo fighting these unauthorized charges.

136. Plaintiff Acree has experienced additional actual fraud as a result of this breach in the form of someone using her personal information to open a bank account with Capital One in January 2022. In March 2022, the account was closed due to inactivity.

137. Plaintiff Acree has noticed an increase in spam phone calls, texts, and emails since approximately October 2021. Plaintiff has noticed that some of these are related to medical care, devices, etc., while others are general spam. Plaintiff Acree no longer answers calls with numbers that she does not recognize.

138. The Data Breach has caused Plaintiff Acree to suffer significant anxiety, anger, and fear due to concerns for future identity theft.

139. Plaintiff Acree plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as, monitoring her credit and identity, and checking her financial accounts more frequently.

Plaintiff Cindy Beaver

140. Plaintiff Beaver used MHS's services over the course of her lifetime, for various care and treatment. To receive services at MHS, Plaintiff Beaver was required to provide her Sensitive Information directly to Defendant's database, which is maintained by Defendant.

141. Plaintiff Beaver greatly values her privacy and Sensitive Information, especially when receiving medical services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her Sensitive Information.

142. Recognizing the substantial risk Plaintiff Beaver faces from the Data Breach, Defendant provided Plaintiff Beaver a one-year subscription to a credit monitoring service. However, Plaintiff Beaver did not opt to use these services, because she was implementing a credit freeze and did not feel it was necessary to use these services.

143. Since learning of the Data Breach, Plaintiff Beaver has spent significant time reviewing her financial accounts, researching the data breach, and has also spent time speaking with her bank regarding her missing funds from her account.

144. Plaintiff Beaver has experienced actual fraud in the form of her Social Security Check missing from her bank account. Plaintiff Beaver spent time on the phone with her bank dealing with the fraudulent activity and was able to have the bank reimburse her for the missing funds.

145. Plaintiff Beaver has spent significant time contacting all three credit bureaus to put a credit freeze on her accounts.

146. Plaintiff Beaver has noticed an increase in spam phone calls and text messages since the fall of 2021. Plaintiff Beaver does not answer calls that come from numbers that she does not recognize but receives numerous calls and text messages a day.

147. The Data Breach has caused Plaintiff Beaver to suffer significant uneasiness, fear, and nervousness due to concerns for future identity theft. In addition, Plaintiff Beaver feels bombarded with the overwhelming amount of spam phone calls and text messages that she now receives as a result of the breach.

148. Plaintiff Beaver plans on taking additional time-consuming, yet necessary, steps to help mitigate the harm caused by the Data Breach, such as, monitoring her credit and identity, and checking her financial accounts more frequently.

CLASS ACTION ALLEGATIONS

149. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

150. Plaintiffs proposes the following Class definitions, subject to amendment as appropriate:

> All persons who utilized MHS's services, whose Sensitive Information was maintained on MHS's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class").

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

152. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time,

based on information and belief, the Class consists of approximately 216,478 individuals whose sensitive data was compromised in the Data Breach.

153. 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 Plaintiffs' and Class Members' Sensitive 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 including, e.g., HIPAA and the FTC Act;

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

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

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

g. Whether computer hackers obtained Class Members' Sensitive Information in the Data Breach;

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

i. Whether Plaintiffs and Class Members suffered legally cognizable injuries as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;

l. Whether Defendant breached express or implied contracts with Plaintiffs and Class Members;

m. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

o. Whether Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages, and/or injunctive relief.

154. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

155. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating Class actions.

156. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer system 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.

157. 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. 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.

158. 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.

CAUSES OF ACTION

COUNT I

Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

159. All other paragraphs are fully re-alleged and incorporated herein.

160. Defendant required patients, including Plaintiffs and Class Members, to submit non-public Sensitive Information in the ordinary course of rendering healthcare services.

161. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Sensitive 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 they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

162. Defendant owed a duty of care to Plaintiffs 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 Sensitive Information.

163. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, state law, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach and data breach.

164. 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 of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

165. 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.

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

167. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Sensitive 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' Sensitive Information;

b. Failing to adequately monitor the security of its IT system;

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

d. Failure to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Sensitive Information; and,

f. 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.

168. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Sensitive 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.

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

170. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

171. Plaintiffs 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) continue to provide adequate credit monitoring to all Class Members.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

172. All other paragraphs are fully re-alleged and incorporated herein.

173. Pursuant to 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 Plaintiffs' and Class Members' Sensitive Information.

174. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Sensitive Information.

175. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it 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" (45 CFR 164.304 definition of encryption).

176. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' Sensitive Information.

177. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act, HIPAA, and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and

Class Members' Sensitive Information.

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

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

180. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Sensitive Information.

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

COUNT III

Breach of Express Contract
(On Behalf of Plaintiffs and the Nationwide Class)

182. All other paragraphs are fully re-alleged and incorporated herein

183. Plaintiffs and Members of the Class allege that they entered into valid and enforceable express contracts with Defendant.

184. The valid and enforceable express contracts that Plaintiffs and Class Members entered into with Defendant include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

185. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class

Members; and (b) protectPlaintiffs' and the Class Members' Sensitive Information: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Sensitive Information.

186. Both the provision of healthcare and the protection of Plaintiffs' and Class Members' Sensitive Information were material aspects of these contracts.

187. At all relevant times, Defendant expressly represented in its Privacy Notice that it would, among other things: a) "maintain the privacy of protected information;" b) "release the minimum amount of your information necessary" and; c) "obtain your written authorization to use or disclose your health information for reasons other than those described in this notice."

188. At least one of these promises embodied in the Privacy Notice (the promise to "release the minimum amount of your information necessary") is not a promise required to be in the Privacy Notice by HIPAA regulations.

189. Defendant's express representations, including, but not limited to, express representations found in its Privacy Notice, formed an express contract requiring Defendant's to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Sensitive Information.

190. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Sensitive Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry-standard data security protocols to protect Sensitive Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class Members would not have entered into these contracts with Defendant and/or its affiliated

healthcare providers without an understanding that their Sensitive Information would be safeguarded and protected.

191. A meeting of the minds occurred, as Plaintiffs and Members of the Class provided their Sensitive Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their Sensitive Information.

192. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Sensitive Information.

193. Defendant materially breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

194. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Sensitive Information as evidenced by its notifications of the Data Breach to Plaintiffs and approximately 216,478 Class Members. Specifically, Defendant did not comply with industry standards, or otherwise protect Plaintiffs' and Class Members' Sensitive Information, as set forth above.

195. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

196. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount

at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

197. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

198. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the compromise of their Sensitive Information, the loss of control of their Sensitive Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

199. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV

Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

200. All other paragraphs are fully re-alleged and incorporated herein.

201. When Plaintiffs and Class Members provided their Sensitive Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

202. Defendant solicited and invited Class Members to provide their Sensitive Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offer and provided their Sensitive Information to Defendant.

203. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant federal and state laws and regulations and were consistent with industry standards.

204. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Defendant include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

205. Under these implied contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' Sensitive Information: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Sensitive Information.

206. Both the provision of healthcare and the protection of Plaintiffs' and Class Members' Sensitive Information were material aspects of these implied contracts.

207. At all relevant times, Defendant expressly represented in its Privacy Notice that it would, among other things: a) "maintain the privacy of protected information;" b) "release the minimum amount of your information necessary" and; c) "obtain your written authorization to use or disclose your health information for reasons other than those described in this notice."

208. At least one of these promises embodied in the Privacy Notice (the promise to "release the minimum amount of your information necessary") is not a promise required to be in the Privacy Notice by HIPAA regulations.

209. Defendant's express representations, including, but not limited to, express representations found in its Privacy Notice, memorialized the mutual assent and meeting of the

minds between Plaintiffs, Class Members, and Defendant, and is part of the implied contract requiring Defendant's to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Sensitive Information.

210. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Sensitive Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class Members would not have entered into these implied contracts with Defendant and/or its affiliated healthcare providers without an understanding that their Sensitive Information would be safeguarded and protected.

211. A meeting of the minds occurred, as Plaintiffs and Members of the Class provided their Sensitive Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their Sensitive Information.

212. Plaintiffs and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security but Defendant failed to do so.

213. Plaintiffs and Class Members would not have entrusted their Sensitive Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Sensitive Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

214. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

215. Through its myriad failures to provide the promised level of data security and protection alleged previously herein, Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Sensitive Information.

216. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

217. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of MHS's computer property and Plaintiffs' and Class Members' Sensitive Information. Thus, Plaintiffs and Class Members did not get what they paid for and contractually agreed to.

218. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

219. Plaintiffs 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.

COUNT V

Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class)

220. All other paragraphs are fully re-alleged and incorporated herein.

221. In light of the special relationship between Defendant and Plaintiffs and Class

Members, whereby Defendant became a guardian of Plaintiffs' and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Sensitive Information; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) maintain complete and accurate records of what patient information (and where) Defendant did and does store.

222. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, in particular, to keep secure the Sensitive Information of its patients.

223. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to adequately protect against cybersecurity events and give notice of the Data Breach in a reasonable and practicable period of time.

224. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the IT systems containing Plaintiffs' and Class Members' Sensitive Information.

225. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

226. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by 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).

227. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by 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).

228. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

229. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

230. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

231. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

232. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

233. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its

workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

234. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

235. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Sensitive Information.

236. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, as described above.

COUNT VI

Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

237. All other paragraphs are fully re-alleged and incorporated herein, except those contained in Counts III and IV (breach of express and breach of implied contract) as this count is plead in the alternative to those counts.

238. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant money for healthcare services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' Sensitive Information, and by providing Defendant with their valuable Sensitive Information.

239. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Sensitive Information, instead of providing a reasonable level of security that would have prevented the Data Breach.

240. Defendant calculated to avoid its data security obligations at the expense of

Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

242. Defendant acquired the monetary benefit and Sensitive Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

243. If Plaintiffs and Class Members knew that Defendant had not secured their Sensitive Information, they would not have agreed to provide their Sensitive Information to Defendant.

244. Plaintiffs and Class Members have no adequate remedy at law.

245. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, as described above.

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

COUNT VII
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

247. All other paragraphs are fully re-alleged and incorporated herein.

248. Under the Declaratory Judgment Act, 28 U.S.C. §2201, *et seq.*, the Court is

authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

249. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its users' Sensitive Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Sensitive Information. Plaintiffs and Class Members remain at imminent risk that further compromises of their Sensitive Information will occur in the future. This is true even if they (or their healthcare providers) are not actively using Defendant's products or services.

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

a. Defendant continues to owe a legal duty to secure users' Sensitive Information and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class Members' Sensitive Information.

251. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Defendant to employ adequate security practices consistent with law and industry standards to protect its users' Sensitive Information.

252. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendant. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs

and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

253. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs to Defendant, Plaintiffs and Class Members will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

254. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach to Defendant, thus eliminating additional injuries that would result to Plaintiff, Class Members, and the millions of other Defendant customers whose Sensitive Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for judgment as follows:

A. For an Order certifying this action as a Class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Sensitive Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and

policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;;

E. For equitable relied providing a full accounting of type of data and the method of unauthorized access, disclosure and acquisition of the Sensitive Information;

F. Ordering Defendant to pay for not less than five years of credit monitoring and identity theft insurance services for Plaintiffs and the Class;

G. For an award of actual damages, compensatory damages, and nominal damages, in an amount to be determined, 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. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: April 29, 2022

Respectfully submitted,

/s/ Terence R. Coates
MARKOVITS, STOCK & DEMARCO, LLC
Terence R. Coates (0085579)
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Joseph M. Lyon (0076050)
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Gary E. Mason (*pro hac vice forthcoming*)
MASON, LLP
5101 Wisconsin Ave., NW, Suite 305
Washington, DC 20016
Phone: 202.640.1160
gmason@masonllp.com

Jeffrey S. Goldenberg (0063771)
GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Phone: (513) 345-8297
Fax: (513) 345-8294
jgoldenberg@gs-legal.com

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on April 29, 2022, the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

*/s/ Terence R. Coates*_____
Terence R. Coates (0085579)

EXHIBIT 1

MARIETTA AREA HEALTH CARE INC. DBA MEMORIAL HEALTH SYSTEM PROVIDES NOTICE OF DATA PRIVACY EVENT
January 12, 2022

Marietta Area Health Care Inc. dba Memorial Health System ("MHS") is providing notice of an incident that could affect the privacy of information of certain patients for whom it provided medical care. While MHS is unaware of any actual or attempted misuse of this information, MHS takes this incident very seriously and is providing information about the incident, our response to it, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On August 14, 2021, MHS identified the presence of malware on certain servers in our environment. We immediately commenced an investigation to determine the full nature and scope of the incident and to secure our network. Through this investigation, we determined that in connection with the malware event, an unauthorized actor accessed certain systems within our network on or about July 10 through August 15, 2021. On or about September 17, 2021, we determined the unauthorized actor may have accessed or acquired information from systems potentially containing patient information. We then carefully reviewed the contents of the affected systems to determine what, if any, sensitive information may have been compromised. On November 1, 2021, our review confirmed the scope of the information at risk and the population potentially impacted. We worked diligently since this time to confirm the patients who may be impacted, the types of information at issue, and the best contact information for the impacted population, in order to provide an accurate notification. On December 9, 2021, our review confirmed the impacted population and we began providing notice to affected individuals.

What Information Was Involved? We conducted a thorough review of the relevant systems to identify the types of information stored there and to whom it related. Our review determined that sensitive information was present in the affected systems and it is possible that this information could have been accessed or acquired by an unauthorized actor. While the specific data elements vary for each potentially affected individual, the scope of information potentially involved includes: name, date of birth, medical record numbers, patient account numbers, Social Security numbers, and other treatment and medical information. Although we have no reason to believe that any identity theft or unauthorized use of the affected information occurred, we wanted to provide notice of this incident.

How Will Individuals Know If They Are Affected By This Incident? We are mailing notice letters to the individuals identified as impacted. If an individual does not receive a letter but would like to know if they are affected, they may call our dedicated assistance line, detailed below.

What MHS is Doing. We have strict security measures to protect the information in our possession and have worked to add further technical safeguards to our environment. Following this incident, we took immediate steps to improve the security of our environment and increase our security posture.

Whom Should Individuals Contact For More Information? If individuals have questions or would like additional information, they may call our dedicated assistance line at (855) 545-2370 between the hours of 9:00 a.m. and 6:30 p.m., Eastern Standard Time, Monday through Friday.

What You Can Do? We encourage individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit

freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

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

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

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. MHS is located at 401 Matthew Street, Marietta, OH 45750.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights

pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 6 Rhode Island residents impacted by this incident.

EXHIBIT 2

Memorial Health System Notice of Privacy Practices

As Required by the Privacy Regulations Created as a Result of the
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Effective: April 1st, 2013

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Memorial Health System, DBA Marietta Memorial and Selby General Hospitals, uses health information about you for treatment, to obtain payment for treatment, for administrative purposes, and to evaluate the quality of care that you receive. Your health information is contained in a medical record that is the physical property of Memorial Health System.

How We May Use and Disclose Medical Information About You

For Treatment: We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, technicians, or others who need to know about you to provide quality patient care. This information may be disclosed through information we record in your medical record or verbally between health care providers. We will also provide other medical facilities with information about you and your diagnoses which they will need in order to treat you.

For Payment: We may use and disclose medical information about you so that the treatment and services you receive may be billed and payment may be collected from you, an insurance company or a third party. For example, we may need to give your insurance company information about a procedure we performed so we can be paid for the procedure.

For Health Care Operations: We may use and disclose medical information about you for operational purposes. For example, your health information may be disclosed to members of the medical staff, risk or quality improvement personnel, and others to evaluate the performance of our staff, assess the quality of care, learn how to improve our facility and services.

Appointments. We may use your information to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

Fund Raising. Memorial Health Foundation may use your information to contact you to raise funds for Memorial Health System and its health related activities. We would only release contact information such as your name, address and phone number and the dates you received treatment or services at the hospital. If you do not want the Foundation to contact you for fundraising efforts, you must notify the Memorial Health Foundation Office.

Hospital Directory. We may include certain limited information about you in the hospital directory while you are a patient at the hospital. This information may include your name, location in the hospital, your general condition (undetermined, good, fair, serious, critical) and your religious affiliation.

Special Situations in Which Your Information May be Released
(including in response to Federal State or Local Law)

- for judicial administrative proceedings pursuant to legal authority;
- to report information related to victims of abuse, neglect or domestic violence and to assist law enforcement officials in their law enforcement duties;
- if necessary to reduce or prevent a serious threat to your health or safety or the health or safety of another person or the public.
- in response to appropriate military authorities if you are a member of the military (including veterans)

Local Public Health Authorities

- in reporting child or elder abuse and neglect
- in reporting communicable diseases or your potential exposure to such
- in notifying you of recalls of drugs, products or devices you may be using

Deceased Patients

- to a medical examiner or coroner to identify a deceased individual or to identify the cause of death
- to allow funeral directors to do their jobs.

Organ/Tissue donation. Your health information may be used or disclosed for cadaveric organ, eye or tissue donation purposes.

Workers' Compensation. Your health information may be used or disclosed in order to comply with laws and regulations related to Workers' Compensation.

We Will Always Get Your Written Authorization Before Releasing or Using Your Information:

- for marketing purposes
- in a manner that would constitute the sale of your protected health information
- in a manner not described in this notice and where required by either Federal or State Law.

Your Health Information Rights

You have a right to:

- request a restriction on certain uses and disclosures of your information as provided by *45 CFR §164.522.* This may include a limit on medical information we disclose about you to someone who is involved in your care or payment for your care, such as a family member or friend. We are, however, not required to agree to a requested restriction except in cases where you have paid your bill in full and requested a restriction on releasing your information to a group health plan, insurer, or other payor for purposes of payment or health care operations. You may request a restriction by completing a form developed by the hospital, or you can send a written request to our Medical Records Department.

- obtain a paper copy of this notice at any time from the Registration Departments at Memorial Health System.
- amend your health record as provided in *45 CFR §164.526.* To request a copy or to amend your information you must make your request in writing to the Medical Records Department.
- request communications of your health information by alternative means or at alternative locations.
- revoke special authorizations to use or disclose health information for certain purposes except to the extent that action has already been taken.
- request an accounting of all disclosures of your health information when the disclosure has not been pursuant to treatment, payment, operations, or an authorization and, if your information is maintained in an electronic format, request an accounting of any disclosures dating back three years from the date of the request.
- inspect or receive a hard copy or an electronic copy of your medical information in a format requested by you if such format is readily producible.
- receive a written notification of any inappropriate release or use of your protected health information.

Obligations of Memorial Health System

We are required to:

- maintain the privacy of protected health information.
- provide you with this notice of our legal duties and privacy practices with respect to your health information.
- abide by the terms of this notice.
- notify you of certain breaches or the inappropriate use or release of your information.
- notify you if we are unable to agree to a requested restriction on how your information is to be used or disclosed.
- accommodate reasonable requests you may make to communicate health information by alternative means or at alternative locations.
- release the minimum amount of your information necessary to accomplish information related functions and de-identify your information to the extent practicable.
- obtain your written authorization to use or disclose your health information for reasons other than those listed above and permitted under law.

Changes to This Notice

We reserve the right to change our information practices and to make new provisions effective for all protected health information we maintain. At the end of this notice you will be asked to sign that you have received the notice and have had the opportunity to receive a copy. Your signature is requested to help us determine which version of the notice you have received. Revised notices will be posted in the Registration Areas, Outpatient Center, Billing Office and our Web Site and a paper copy will be made available to you upon request.

If you have questions or complaints, please contact:

Memorial Health System Patient Representative
401 Matthew Street
Marietta, OH 45750
740-374-1541

If you believe your privacy rights have been violated, you can file a complaint with the Memorial Health System Patient Representative or with the Department of Health and Human Services. There will be no retaliation for filing a complaint.

ACKNOWLEDGMENT

_____ DATE

_____ Signature of Patient

_____ Other Person Legally Authorized to Acknowledge

_____ Relationship to Patient

MMH USE ONLY

Reason acknowledgment was not obtained: