IN THE PENNSYLVANIA COURT OF COMMON PLEAS
WARREN COUNTY

ROBERT PESSIA, PETER HETTMAN, HEIDI TULLER, ROBERT MARRONE, and JEAN BERRY individually and on behalf of all others similarly situated, Plaintiffs, v. WARREN GENERAL HOSPITAL, Defendant.	CIVIL DIVISION CASE NO. 501 - 23 **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** CONSOLIDATED CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

1. Plaintiffs Robert Pessia, Peter Hettman, Heidi Tuller, Robert Marrone, and Jean Berry ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant Warren General Hospital ("WGH" or "Defendant") seeking damages, restitution, and injunctive relief. 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

2. This class action arises out of Defendant WGH's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiffs' and Class Members' sensitive personal identifiable information ("PII") and protected health information ("PHI" and, collectively with PII, the "Private Information") that it acquired and stored for its business purposes. This failure to secure and monitor its network resulted in a September 2023 data breach ("Data Breach" or "Breach") of highly sensitive documents and information stored on the computer network of

WGH, an organization that provides medical treatment and/or employment to individuals, including Plaintiffs and Class Members.

3. Defendant's data security failures allowed a targeted cyberattack in or about September 2023 to compromise Defendant's network resulting in the exfiltration of Plaintiffs and other individuals ("the Classes") Private Information.

4. According to a notice WGH sent to the Department of Health and Human Services Office for Civil Rights ("HHS") on or about November 9, 2023, as of that date, it identified the Breach having affected 168,921 individuals.[1]

5. According to a notice on its website, Defendant confirmed that a "data security event" occurred on its network between September 15, 2023 and September 23, 2023.

6. Defendant's website notice states: "The investigation determined that an unknown actor accessed certain computer systems in our network between September 15, 2023, and September 23, 2023, and downloaded certain information from our network. In response, we undertook a comprehensive review of our internal records to determine what information was present on the affected systems and identified contact information to provide notification to potentially impacted individuals. We recently completed our review."[2]

7. Despite learning of the Data Breach on or about September 24, 2023 and determining that Private Information was compromised in the Breach occurring from September 15, 2023 to September 23, 2023, Defendant did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until November 17, 2023.

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Feb. 28, 2024).

[2] https://www.wgh.org/data (last accessed Feb. 28, 2024).

8. The Private Information compromised in the Data Breach included the Private Information of current and former employees and patients, including Plaintiffs. This Private Information included, but is not limited to names, addresses, dates of birth, Social Security numbers, financial account information, payment card information, health insurance claims information, and medical information including diagnoses, medications, lab results, and other treatment information.[3]

9. The Private Information compromised in what WGH refers to as a "data security event" in which it "identified suspicious activity on [its] network."[4] In other words, the cybercriminals intentionally targeted WGH for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then exfiltrated highly sensitive Private Information, including but not limited to Social Security numbers. As a result, the Private Information of Plaintiffs and the Classes remains in the hands of those cyber-criminals.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for either treatment or employment or both.

11. Plaintiffs bring this class action lawsuit individually and on behalf of all others similarly situated to address Defendant's implementation of inadequate controls and safeguards resulting in a hacker gaining access to, and exfiltrating, the Private Information of Plaintiffs and Class Members, and Defendant's failure to provide timely and adequate notice to Plaintiffs and other Class Members that their Private Information had been subject to the unauthorized access of

---

[3] *Id.*

[4] *See* Notice Letter, https://www.mass.gov/doc/assigned-data-breach-number-30976-warren-general-hospital-11-17-23/download (last accessed Feb. 28, 2024) ("Notice Letter").

an unknown third party and including in that notice precisely what specific types of information were accessed and taken by cybercriminals.

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

13. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently implementing and maintaining inadequate cybersecurity policies, tools, measures, and controls to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

14. In addition, Defendant WGH failed to properly monitor the computer network and systems that housed the Private Information. Had WGH properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals almost a month of unimpeded access to the Private Information of Plaintiffs and Class Members.

15. Armed with the Private Information accessed in the Data Breach, data thieves can and do commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information,

filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. As a result of Defendant's conduct, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

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

18. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

19. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence; (ii) breach of contract; (iii) breach of implied contract; (iv) breach of fiduciary duty; (v) breach of confidences; (vi) unjust enrichment; (vii) violations of the Pennsylvania Unfair Trade Practices and Consumer Protection law; and (viii) declaratory relief.

20. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

21. Plaintiff Robert Pessia is a resident and citizen of the state of Texas. Plaintiff Pessia received a letter dated November 17, 2023 from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Defendant's network and systems, which included Plaintiff's Private Information. The compromised files contained the names, dates of birth, addresses, financial account information, payment card information, health insurance claims information, Social Security Numbers, and medical information that Defendant obtained in connection with its business operations.

22. Plaintiff Peter Hettman is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff Hettman received a letter dated November 17, 2023 from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Defendant's network and systems, which included Plaintiff's Private Information. The compromised files contained the names, dates of birth, addresses, financial account information, payment card information, health insurance claims information, Social Security Numbers, and medical information that Defendant obtained in connection with its business operations.

23. Plaintiff Heidi Tuller is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff Tuller received a letter dated November 17, 2023 from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Defendant's network and systems, which included Plaintiff's Private Information. The compromised files contained the names, dates of birth, addresses, financial account information, payment card information, health insurance claims information, Social Security Numbers, and medical information that Defendant obtained in connection with its business operations.

24. Plaintiff Robert Marrone is, and at all times relevant, a resident and citizen of the Commonwealth of Pennsylvania, living in Warren County. Plaintiff received a letter dated November 17, 2023 from Defendant regarding the Data Breach. The letter stated that unauthorized actors gained access to files on Defendant's network and systems, which included Plaintiff's Private Information. WGH advised Plaintiff that the type of his information that may have been impacted included his name, address, date of birth, Social Security number, financial account information, payment card information, health insurance claims information, and medical information including diagnosis, medications, lab results, and other treatment information.

25. Plaintiff Jean Berry is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff Berry received a letter dated November 17, 2023 from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Defendant's network and systems, which included Plaintiff's Private Information. The compromised files contained the names, dates of birth, addresses, financial account information, payment card information, health insurance claims information, Social Security Numbers, and medical information that Defendant obtained in connection with its business operations.

26. Warren General Hospital is a Pennsylvania non-profit corporation that has its principal place of business at 2 Crescent Park West, Warren, Pennsylvania 16365. It can be served through its registered agent at its principal place of business.

JURISDICTION AND VENUE

27. This Court has jurisdiction over this matter pursuant to 42 Pa. C.S. § 931.

28. This Court has subject matter jurisdiction over this action because the events and conduct giving rise to the claims brought in this Complaint occurred in large part in this County.

29. This Court has personal jurisdiction over Defendant pursuant to 42 Pa. C.S. § 5301 because it is a Pennsylvania domestic nonprofit corporation, with its significant business operations and real property located in this County.

30. Venue is proper in this County under Pa. R.C.P. § 1006(a)(1) because of Warren General Hospital's operations in this County, and because a substantial part of the events or omissions giving rise to the claim arose here.

FACTUAL ALLEGATIONS

Defendant's Business

31. Defendant Warren General Hospital "is a community-centered hospital that was constructed in response to the community's need for expanded healthcare services."[5] The hospital opened in 1900 and has since expanded to include more areas of care and clinics on the premises.

32. WGH's services include "a wide range of medical services, including emergency care, surgery, rehabilitation, and specialized treatments."[6]

33. For the purposes of this Class Action Complaint, all of WGH's associated locations will be referred to collectively as "WGH."

34. In the ordinary course of receiving medical care services from Defendant WGH, or alternatively being employed by WGH, each patient and employee must provide (and Plaintiffs did provide) Defendant WGH with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;

[5] https://www.wgh.org/history (last accessed Feb. 28, 2024).

[6] https://www.wgh.org/about (last accessed Feb. 28, 2024).

- Marital status;
- Employer with contact information;
- Primary and secondary insurance policy holders' name, address, date of birth, and Social Security number;
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

35. Defendant also creates and stores medical records and other protected health information for its patients, records of treatments and diagnoses.

36. By obtaining, collecting, receiving, and/or storing Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

37. Plaintiffs and Class Member transferred their Private Information—which is valuable private property—to Defendant for the purposes of facilitating services from and employment with Defendant and with the agreement and understanding that the Private Information would be adequately safeguarded and/or destroyed within a reasonable time after the termination of the relationship thereby creating a bailment.

38. Upon information and belief, WGH's HIPAA Notice of Privacy Practices ("Privacy Policy") is provided to every patient both prior to receiving treatment and upon request.[7] WGH's Privacy Notice makes clear that it understands that its patients' Private Information is personal and must be protected by law.

39. In its Privacy Policy, WGH states that:

a. Patients' have the right to "[p]rivacy concerning your own medical care."

b. Patients' have the right to "[h]ave all records pertaining to your medical care treated as confidential."

c. "Patients will receive services and care that are... required by law and regulation."

d. Private Information will be disclosed only in certain circumstances, none of which include circumstances like the Data Breach.[8]

40. Defendant WGH agreed to and undertook legal duties to maintain the protected health and Private Information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

41. The patient information held by Defendant WGH in its computer system and network included the highly sensitive Private Information of Plaintiffs and Class Members.

---

[7] https://www.wgh.org/patients-rights-respon-and-privacy (last accessed Feb. 21, 2024); https://static1.squarespace.com/static/64011f10da897a3162ea8900/t/64aeca857c684b7713fd4849/1689176710313/Patients-+Rights-No-Watermark.pdf, attached as Exhibit A.

[8] *Id.*

42. Yet, through its failure to properly secure the Private Information of Plaintiffs and Class, WGH failed to meet its own duties and promises of patient privacy.

43. Upon information and belief, Defendant does not follow its own policies or industry standard practices in securing Private Information.

44. Upon information and belief, Defendant failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.[9]

45. Upon information and belief, Defendant failed to ensure the proper monitoring and logging of file access and modifications.[10]

46. Upon information and belief, Defendant failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.[11]

47. Upon information and belief, Defendant failed to ensure the proper encryption of Plaintiffs' and Class Members' Private Information.[12]

48. Upon information and belief, Defendant inadequately trains its employees and cybersecurity partners on cybersecurity policies and then fails to enforce those policies.

49. Upon information and belief, Defendant failed to maintain reasonable and adequate security practices over its systems storing Plaintiffs' and Class Members' Private Information.

---

[9] *See* Notice Letter, https://www.mass.gov/doc/assigned-data-breach-number-30976-warren-general-hospital-11-17-23/download (last accessed Feb. 28, 2024) (noting that although the Breach began on September 15, 2023 (including unauthorized network access and file "download"), WGH did not identify suspicious activity until nine days later on September 24, 2023).

[10] *Id.* (noting that, even "after a comprehensive review of [] internal records," WGH is uncertain as to which files and information were accessed or downloaded and stating only that certain files "may" have been present on impacted systems).

[11] *Id.*

[12] *Id.* (noting that Private Information was downloaded).

50. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties.

51. If Defendant had adopted reasonable measures to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties, for example, properly encrypting Plaintiffs' and Class Members' Private Information, the Breach would not have occurred or at minimum, its effects and Plaintiffs' and Class Members' injuries would have been mitigated.[13]

The Data Breach

52. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like WGH.

53. According to Defendant's website Notice, it learned of "suspicious activity" on its computer systems that occurred around September 15, 2023 through September 23, 2023, when "an unknown actor accessed certain computer systems in [its] network."[14]

54. Defendant notified HHS of the Data Breach on or about November 9, 2023, listing 168,921 victims affected.

55. In January 2023, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like WGH of the severe threats posed by Royal, BlackCat and similar cybercriminal groups.[15] Within the healthcare industry, the risk of a cyber-attack is well-known and preventable with adequate security systems in place.

---

[13] *Id.* (noting that, after discovering the Breach, WGH took action to "reduce the likelihood of a similar future event").

[14] *See* Notice Letter, https://www.mass.gov/doc/assigned-data-breach-number-30976-warren-general-hospital-11-17-23/download (last accessed Feb. 28, 2024).

[15] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last accessed Feb. 28, 2024).

56. On or about November 17, 2023, months after WGH learned that the Class's Private Information was attacked by cybercriminals, WGH patients began receiving their notices of the Data Breach informing them that its investigation determined that their Private Information was accessed.

57. WGH's notice letters list time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing one year of credit monitoring that Plaintiffs and Class Members would have to affirmatively sign up for and a call center number that victims may contact with questions, WGH offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, WGH sent a similar generic letter to all other individuals affected by the Data Breach.

58. WGH's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

59. WGH knew or should have known that its electronic records would be targeted by cybercriminals.

60. WGH had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

The Data Breach was a
Foreseeable Risk of which Defendant was on Notice.

62. It is well known that Private Information, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including WGH, are well-aware of the risk of being targeted by cybercriminals.

63. Individuals place a high value not only on their Private Information, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

64. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss." [16]

65. Individuals, like Plaintiffs and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

---

[16] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Feb. 28, 2024).

66. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

67. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[17]

68. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[18]

69. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[19]

---

[17] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Feb. 28, 2024).

[18] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed Feb. 28, 2024).

[19] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed Feb. 28, 2024).

70. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

71. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [20] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[21]

72. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Private Information private and secure, WGH failed to take appropriate steps to protect the Private Information of Plaintiffs and the proposed Class from being compromised.

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

74. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year.

---

[20] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed Feb. 28, 2024).

[21] *Id.*

2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[22]

75. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[23]

76. The HIPAA Journal article goes on to explain that patient records, like those stolen from WGH, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[24]

77. Data breaches such as the one experienced by Defendant WGH 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, can prepare for, and hopefully can ward off a potential attack.

---

[22] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed Feb. 28, 2024).

[23] *Id.*

[24] *Id.*

78. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[25]

79. HHS data shows more than 39 million patients' information was exposed in the first half of 2023 in nearly 300 incidents and that healthcare beaches have doubled between 2020 and 2023, according to records compiled from HHS data by Health IT Security.[26]

80. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[27]

81. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant WGH.

Defendant Fails to Comply with FTC Guidelines.

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

83. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.

---

[25] *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 accessed Feb. 28, 2024).

[26] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (last accessed Feb. 28, 2024).

[27] https://www.ahu.edu/blog/data-security-in-healthcare (last accessed Feb. 28, 2024).

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.[28] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[29]

84. 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.

85. The FTC has brought enforcement actions against businesses, like that of WGH, 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.

86. 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,

---

[28] *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 accessed Feb. 28, 2024).

[29] *Id.*

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.").

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

88. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

89. Defendant was at all times fully aware of its obligation to protect the Private Information of its patients and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards.

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

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

92. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such

as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

93. 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.

94. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and failing to thwart the Data Breach.

Defendant's Conduct Violates HIPAA.

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

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

97. 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).

98. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

99. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Defendant Breached its Duties to Plaintiffs and Class.

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

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

b. Failing to adequately protect patients' Private Information;

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

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

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

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

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

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

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

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

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

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI 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).

101. Defendant also breached its duty of confidence to its patients by failing to maintain the privacy of patients' medical records.

102. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

103. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft.

104. Data Breaches such as the one experienced by Plaintiffs and the Classes are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

105. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[30] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the

[30] https://www.gao.gov/assets/gao-19-230.pdf (last accessed Feb. 28, 2024).

consumers' options. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiffs and the Classes) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

106. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report"). [31]

107. The FTC like the GAO, 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 (consider 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.[32]

108. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

109. 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; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

---

[31] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed Feb. 28, 2024) ("2007 GAO Report").

[32] *See* https://www.identitytheft.gov/Steps (last accessed Feb. 28, 2024).

110. Theft of Private Information is also gravely serious. Private Information is a valuable property right.[33]

111. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies 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 2007 GAO Report, at p. 29.

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

113. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[34]

---

[33] *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).

[34] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone

114. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a "Fullz" package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members.

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

116. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[35]

---

with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm, Krebs On Security, https://krebsonsecurity.com/tag/fullz/ (last accessed Feb. 5, 2024).

[35] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last accessed Feb. 28, 2024).

117. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[36] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social 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.[37] 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.

118. 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."[38]

119. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card

---

[36] *Identity Theft and Your Social Security Number*, Social Security Administration (last accessed March 16, 2023). (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Feb. 28, 2024).

[37] *Id.* at 4.

[38] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Feb. 28, 2024).

information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[39]

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

PLAINTIFFS' EXPERIENCES

Plaintiff Robert Pessia

121. Plaintiff Robert Pessia is and was a patient of Defendant. As a condition to receiving medical services, Plaintiff Pessia was required to and Plaintiff provided his Private Information to Defendant which was then entered into Defendant's systems and maintained on its network.

122. Plaintiff Pessia greatly values his privacy and Private Information, especially when submitting information related to health care. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of his Private Information, e.g., Plaintiff Pessia stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; moreover, he diligently selects unique usernames and passwords on his various accounts; and he has not knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

---

[39] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Feb. 28, 2024).

123. Plaintiff Pessia received a letter dated November 17, 2023 from Defendant concerning the Data Breach. The letter states that unauthorized actors gained access to files on Defendant's network, which included Plaintiff's Private Information. The compromised files contained the names, dates of birth, social security numbers, and medical information that Defendant obtained in connection with its business operations. Plaintiff Pessia is especially alarmed by the vagueness of his stolen extremely private medical information (PHI) and equally by the fact that his Social Security number was identified as among the breached data on WGH's computer system.

124. Shortly after and as a result of the Data Breach, Plaintiff Pessia became aware that an unauthorized party applied for multiple credit cards in Plaintiff Pessia's name.

125. Shortly after and as a result of the Data Breach, Plaintiff Pessia became aware that approximately 30 unauthorized hard inquires on his credit for auto and other loans were made. As a result, Plaintiff Pessia had to spend considerable time contesting false credit report items, his credit score dropped, and he was unable to obtain financing for a car.

126. Starting in approximately October 2023 and as a result of the Data Breach, Plaintiff Pessia began receiving an excessive number of spam calls every day on the same cell phone number provided to WGH on his records.

127. In addition, Plaintiff Pessia receives *many* spam emails and texts now, which was not typical before the Data Breach. He cannot figure out any other explanation than that it is related to WGH's Data Breach which included his Private Information.

128. Shortly after and as a result of the Data Breach, Plaintiff Pessia was notified that his Social Security number, date of birth, and address had been found on the dark web.

129. Recognizing the present, immediate, and substantial increased risk of harm that Plaintiff Pessia faces, Defendant offered him twelve 12 months of identity theft protection services through CyEx.

130. The Notice letter Plaintiff received also advised Plaintiff Pessia to "remain vigilant against incidents of identity theft and fraud" by reviewing your account information and credit reports for "suspicious activity."

131. Since learning of the Data Breach, Plaintiff Pessia has heeded Defendant's advice and warnings and spent additional time in response to the Data Breach. Specific examples of time spent include that since the Data Breach, Plaintiff Pessia monitors his financial accounts for about an hour per day. This is more time than he spent prior to learning of the WGH's Data Breach. Having to do this every week not only wastes his time as a result of WGH's negligence, but it also causes him great anxiety.

132. As a result of the Data Breach and at the recommendations of WGH, Plaintiff Pessia has frozen his credit, changed his passwords, and monitored his accounts to mitigate the impact of the Data Breach. Plaintiff Pessia spends approximately ten hours a week dealing with issues caused by the Data Breach.

133. Plaintiff Pessia plans on taking additional time-consuming necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing bank, credit and other accounts for unauthorized activity.

134. The Data Breach has caused Plaintiff Pessia to suffer fear, anxiety, and stress, which has been compounded by the fact that WGH has not been forthright about the cause and full scope of the Private Information compromised in the Data Breach.

135. Plaintiff Pessia has lost confidence in his health care provider—WGH—because of its failure to protect his medical records and medical information.

136. Plaintiff Pessia has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches and that the confidentiality of his medical records and information is maintained.

Plaintiff Peter Hettman

137. Plaintiff Peter Hettman is a current patient of Defendant. As a condition to receiving medical services, Plaintiff was required to and Plaintiff provided his PII and PHI to Defendant, which was then entered into Defendant's systems and maintained on its network.

138. Plaintiff Hettman greatly values his privacy and PII, especially when submitting information related to health care providers. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of his PII -- e.g, Plaintiff Hettman stores sensitive documents with PII in safe and secure locations and safely destroys sensitive documents; moreover, he diligently selects unique usernames and passwords on his various accounts; and he has not knowingly transmitted unencrypted PII over the internet or other unsecured source.

139. Plaintiff Hettman received a letter dated November 17, 2023, from Defendant concerning the Data Breach. The letter states that unauthorized actors gained access to files on Defendant's network, which included Plaintiff's PII. The compromised files contained the names, dates of birth, Social Security numbers, and medical information that Defendant obtained in connection with its business operations.

140. Recognizing the present, immediate, and substantial increased risk of harm that Plaintiff Hettman faces, Defendant offered him twelve (12) months of identity theft protection services through CyEx.

141. The letter Plaintiff Hettman received also advised Plaintiff to "remain vigilant against incidents of identity theft and fraud" by reviewing account information and credit reports for "suspicious activity."

142. Since learning of the Data Breach, Plaintiff Hettman has heeded Defendant's advice and warnings and spent additional time monitoring his accounts. Plaintiff spends about an hour per week monitoring his accounts in response to the Data Breach.

143. Plaintiff Hettman plans on taking additional time-consuming necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing bank, credit, and other accounts for unauthorized activity.

144. Plaintiff Hettman reports an increase in other spam calls, text messages, and phishing emails after the Data Breach.

145. The Data Breach has caused Plaintiff Hettman to suffer fear, anxiety, and stress, which has been compounded by the fact that WGH has not been forthright about the cause and full scope of the PII compromised in the Data Breach.

146. Plaintiff Hettman has lost confidence in his health care provider—WGH—because of its failure to protect his medical records and medical information.

147. Plaintiff Hettman has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches and safeguarded from future breaches and that the confidentiality of his medical records and information is maintained.

Plaintiff Robert Marrone

148. Plaintiff Robert Marrone is and was a patient of Defendant. As a condition to receiving medical services, Plaintiff Marrone was required to and Plaintiff provided his Private Information to Defendant which was then entered into Defendant's systems and maintained on its network.

149. Plaintiff Marrone received a letter dated November 17, 2023 from Defendant concerning the Data Breach. The letter states that unauthorized actors gained access to files on Defendant's network, which included Plaintiff's Private Information. The compromised files contained the names, dates of birth, social security numbers, and medical information that Defendant obtained in connection with its business operations. Plaintiff Marrone is alarmed by the vagueness of Defendant's Notice Letter and equally by the fact that his Social Security number was identified as among the breached data on WGH's computer system.

150. Recognizing the present, immediate, and substantial increased risk of harm that Plaintiff Marrone faces, Defendant offered him twelve 12 months of identity theft protection services through CyEx.

151. The Notice letter Plaintiff received also advised Plaintiff Marrone to "remain vigilant against incidents of identity theft and fraud" by reviewing your account information and credit reports for "suspicious activity."

152. Since learning of the Data Breach, Plaintiff Marrone has heeded Defendant's advice and warnings and spent additional time in response to the Data Breach. Plaintiff Marrone has and will take the time-consuming necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing bank, credit, and other accounts for unauthorized activity.

153. Shortly after and as a result of the Data Breach, Plaintiff Marrone was targeted for fraud and identity theft. Specifically, accounts were opened in his name without his authorization or approval. Upon information and belief, third parties obtained Plaintiff Marrone's Private Information and opened these accounts for the purpose of committing further identity theft and fraud, which likely would have been successful but for Plaintiff Marrone's vigilance.

154. Plaintiff Marrone has lost confidence in his health care provider—WGH—because of their failure to protect his medical records and medical information.

155. Plaintiff Marrone is very concerned about his PII and PHI being accessed and exfiltrated by cybercriminals.

156. Plaintiff Marrone has lost confidence in his health care provider—WGH—because of its failure to protect his medical records and medical information.

157. Plaintiff Marrone has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches and that the confidentiality of his medical records and information is maintained.

Plaintiff Heidi Tuller

158. Plaintiff Heidi Tuller is a current patient of Defendant. As a condition to receiving medical services, Plaintiff was required to and Plaintiff provided her PII and PHI to Defendant, which was then entered into Defendant's systems and maintained on its network.

159. Plaintiff Tuller greatly values her privacy and PII, especially when submitting information related to health care providers. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her PII -- *e.g*, Plaintiff stores sensitive documents with PII in safe and secure locations and safely destroys sensitive documents; moreover, she diligently

selects unique usernames and passwords on her various accounts; and she has not knowingly transmitted unencrypted PII over the internet or other unsecured source.

160. Plaintiff Tuller received a letter dated November 17, 2023, from Defendant concerning the Data Breach. The letter states that unauthorized actors gained access to files on Defendant's network, which included Plaintiff's PII. The compromised files contained the names, dates of birth, Social Security numbers, and medical information that Defendant obtained in connection with its business operations.

161. Recognizing the present, immediate, and substantial increased risk of harm that Plaintiff Tuller faces, Defendant offered her twelve (12) months of identity theft protection services through CyEx.

162. Plaintiff Tuller has been forced to be more diligent in her credit monitoring, which includes communications with her financial institution about unauthorized activity.

163. The letter Plaintiff Tuller received also advised Plaintiff to "remain vigilant against incidents of identity theft and fraud" by reviewing account information and credit reports for "suspicious activity."

164. Since learning of the Data Breach, Plaintiff Tuller has heeded Defendant's advice and warnings and spent additional time monitoring her accounts. Plaintiff spends about 10-15 minutes per week monitoring her accounts in response to the Data Breach.

165. Plaintiff Tuller plans on taking additional time-consuming necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing bank, credit, and other accounts for unauthorized activity.

166. Plaintiff Tuller has also noticed an increase in spam calls, text messages, and phishing emails after the Data Breach. In particular, she reports an increase in phishing emails

purporting to be from the credit monitoring service "Experian." As a result, Plaintiff contacts her financial institution directly to obtain a credit report when needed.

167. The Data Breach has caused Plaintiff Tuller to suffer fear, anxiety, and stress, which has been compounded by the fact that WGH has not been forthright about the cause and full scope of the PII compromised in the Data Breach.

168. Plaintiff Tuller has lost confidence in her health care provider—WGH—because of its failure to protect her medical records and medical information.

169. Plaintiff Tuller has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches and that the confidentiality of her medical records and information is maintained.

Plaintiff Jean Berry

170. Plaintiff Berry is a patient of Defendant. As a condition to receiving medical services. Plaintiff was required to and Plaintiff provided her PII and PHI to Defendant which was then entered into Defendant's systems and maintained on its network.

171. Plaintiff Berry greatly values her privacy and PII, especially when submitting information related to (health care providers/employment). Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her PII -- e. g, Plaintiff Berry stores sensitive documents with PII in safe and secure locations and safely destroys sensitive documents; moreover, she diligently selects unique usernames and passwords on her various accounts; and she has not knowingly transmitted unencrypted PII over the internet or other unsecured source.

172. Recognizing the present, immediate, and substantial increased risk of harm that Plaintiff faces, Defendant offered her twelve (12) months of identity theft protection services through CyEx.

173. Plaintiff Berry has signed up for credit monitoring after learning about the fraud.

174. The letter Plaintiff received also advised Plaintiff Berry to "remain vigilant against incidents of identity theft and fraud" by reviewing your account information and credit reports for "suspicious activity".

175. Since learning of the Data Breach, Plaintiff Berry has heeded Defendant's advice and warnings and spent additional time in response to the Data Breach.

176. Plaintiff has also noticed an increase in other spam calls, text messages, and phishing emails after the Data Breach. She receives hundreds of spam emails per day.

177. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that WGH has not been forthright about the cause and full scope of the PII compromised in the Data Breach.

178. Plaintiff Berry has lost confidence in her health care provider—WGH—because of its failure to protect her medical records and medical information.

179. Plaintiff Berry has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches and that the confidentiality of her medical records and information is maintained.

PLAINTIFFS' AND CLASS MEMBERS' INJURIES

180. To date, Defendant WGH has done absolutely nothing to compensate Plaintiffs and Class Members for the damages they sustained in the Data Breach.

181. Defendant WGH has merely offered one year of credit monitoring services through CyEx, a tacit admission that its failure to protect their Private Information has caused Plaintiffs and Class great injuries. *See* Notice Letter. These limited services are inadequate when victims are likely to face many years of identity theft.

182. WGH's offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

183. Furthermore, Defendant WGH's credit monitoring offer and advice (*see* Notice Letter) to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Defendant merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

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

185. Plaintiffs' and Class Members' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

186. Plaintiffs and the Classes were damaged in that their Private Information is now in the hands of cyber criminals, sold and potentially for sale for years into the future.

187. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

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

189. Because of the Data Breach, Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; and 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

190. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of WGH's conduct.

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

192. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those

affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[40]

193. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[41]

194. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[42]

195. Further, the value of Plaintiffs' and Class Members' PII and PHI has been diminished by its exposure in the Data Breach. Plaintiffs and Class Members suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach.

196. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

197. Plaintiffs and Class Members have also been injured by WGH's unauthorized disclosure of their confidential and private medical records and PHI.

198. Plaintiffs and the Class Members have lost confidence in WGH's ability to maintain the confidentiality of their medical records and medical information.

---

[40] https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Feb. 28, 2024).

[41] https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud (last visited Feb. 28, 2024).

[42] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Feb. 28, 2024).

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

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

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

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

g. Placing "freezes" and "alerts" with credit reporting agencies;

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

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

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

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

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

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

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

202. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, WGH knew of the breach since September 24, 2023 and did not notify the victims until November 17, 2023 Yet WGH offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiffs and the Classes.

CLASS ACTION ALLEGATIONS

203. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

204. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

All persons whose Private Information was compromised as a result of the Data Breach discovered by Warren General Hospital in September 2023 and to whom it provided notice in or about November 2023 (the "Class").

All patients of Defendant whose Private Information was compromised as a result of the Data Breach discovered by Warren General Hospital in September 2023 and to whom it provided notice in or about November 2023 (the "Patient Class" and collectively with the "Class", the "Classes").

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

206. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under the 231 Pa. Code Ch. 1700, *et seq.*

207. Numerosity, The Members of the Classes are so numerous that joinder of all of them is impracticable. The number of class members are believed to be around 168,921 people.

208. Commonality. As required by the 231 Pa. Code Ch, 1702(2), there are questions of law and fact common to the Classes, 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' Private Information;

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

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

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

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

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

g. Whether computer hackers obtained Class Members' Private 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 damages as a result of Defendant's misconduct;

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

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

209. Typicality: Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach. Pa. R. Civ. P. 1702(3).

210. Adequacy of Representation, Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Classes. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind. Pa. R. Civ. P. 1702(4).

211. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

212. 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.

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

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

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

b. Whether Defendant owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

g. Whether Defendant failed to abide by its responsibilities under HIPAA.

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

CAUSES OF ACTION

First Count
Negligence
(On Behalf of Plaintiffs and The Classes)

216. Plaintiffs reallege and incorporate paragraphs 1-215 as if fully set forth herein.

217. Defendant WGH required Plaintiffs and Class Members to submit non-public Private Information in order to obtain healthcare/medical services and/or employment.

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

219. 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 Private Information.

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

221. 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 healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

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

224. Plaintiffs and Class Members belong to the class of person that HIPAA was intended to protect.

225. Plaintiffs' and Class Members' injuries are precisely the type of injuries that the HIPAA guards against.

226. 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.

227. Plaintiffs and Class Members belong to the class of person that the FTCA was intended to protect. Plaintiffs' and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

228. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer

systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

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

230. 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 Private Information.

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

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

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

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

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

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; 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.

232. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach

of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

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

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

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

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

Second Count
Breach of Contract
(On Behalf of Plaintiffs and The Classes)

237. Plaintiffs reallege and incorporate paragraphs 1-236 as if fully set forth herein.

238. WGH's Privacy Policy is an agreement between Plaintiffs and Class Members.

239. In its Privacy Policy, WGH agrees to respect patient "[p]rivacy concerning [] medical care," to "treat[] as confidential" " all records pertaining to your medical care," to provide all services, including data security, as " required by law and regulation," and to disclose Private Information only in certain circumstances, none of which include circumstances like the Data Breach.[43]

[43] *Id.*

240. Plaintiffs and Class Members on the one side and WGH on the other formed a contract when Plaintiffs and Class Members obtained products or services from WGH, or otherwise provided Private Information to WGH subject to its Privacy Policy.

241. Plaintiffs and Class Members fully performed their obligations under the contracts with WGH.

242. WGH breached its agreement with Plaintiffs and Class Members by failing to protect their Private Information. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

243. As a direct and proximate result of WGH's breach of contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by WGH; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation

measures because of WGH's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

Third Count
Breach of Implied Contract
(On Behalf of Plaintiffs and The Classes)

244. Plaintiffs reallege and incorporate paragraphs 1-243 as if fully set forth herein.

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

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

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

248. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

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

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

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

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

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

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

255. 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 long-term credit monitoring to all Class Members.

Fourth Count
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and The Patient Class)

256. Plaintiffs reallege and incorporate paragraphs 1-255 as if fully set forth herein.

257. In light of the special relationship between Defendant WGH and Plaintiffs and the Patient Class, whereby Defendant became guardian of Plaintiffs' and the Patient Class's Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and the Patient Class , (1) for the safeguarding of Plaintiffs' and the Patient Class's Private Information; (2) to timely notify Plaintiffs and the Patient

Class of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

258. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and the Patient Class upon matters within the scope of its relationship with its current and former patients and employees to keep secure their Private Information.

259. Defendant breached its fiduciary duties to Plaintiffs and the Patient Class by failing to diligently discover, investigate, and give detailed notice of the Data Breach to Plaintiffs and the Patient Class in a reasonable and practicable period of time.

260. Defendant breached its fiduciary duties to Plaintiffs and the Patient Class by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and the Patient Class Members' Private Information.

261. Defendant breached its fiduciary duties owed to Plaintiffs and the Patient Class by failing to timely notify and/or warn Plaintiffs and the Patient Class Members of the Data Breach.

262. Defendant breached its fiduciary duties to Plaintiffs and the Patient Class Members by otherwise failing to safeguard Plaintiffs' and the Patient Class Members' Private Information.

263. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and the Patient Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk

to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and the Patient Class Members; and (vii) the diminished value of Defendant's services they received.

264. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and the Patient Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

Fifth Count
Breach of Confidences
(On Behalf of Plaintiffs and The Patient Class)

265. Plaintiffs reallege and incorporate paragraphs 1-264 as if fully set forth herein.

266. Plaintiffs and the Patient Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by WGH and that was ultimately accessed or compromised in the Data Breach.

267. As a healthcare provider, WGH has a special relationship to its patients, like Plaintiffs and the Patient Class Members.

268. Because of that special relationship, WGH was provided with and stored private and valuable PHI related to Plaintiffs and the Patient Class, which it was required to maintain in confidence.

269. Plaintiffs and the Patient Class provided WGH with their personal and confidential PHI under both the express and/or implied agreement of WGH to limit the use and disclosure of such PHI.

270. WGH owed a duty to Plaintiffs and the Patient Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

271. WGH had an obligation to maintain the confidentiality of Plaintiffs' and the Patient Class Members' PHI.

272. Plaintiffs and the Patient Class have a privacy interest in their personal medical matters, and WGH had a duty not to disclose confidential medical information and records concerning its patients.

273. As a result of the parties' relationship, WGH had possession and knowledge of confidential PHI and confidential medical records of Plaintiffs and the Patient Class .

274. Plaintiffs' and the Class's PHI is not generally known to the public and is confidential by nature.

275. Plaintiffs and Class Members did not consent to nor authorize WGH to release or disclose their PHI to an unknown criminal actor.

276. WGH breached the duties of confidence it owed to Plaintiffs and the Patient Class when Plaintiffs' and the Patient Class Member's PHI was disclosed to unknown criminal hackers.

277. WGH breached its duties of confidence by failing to safeguard Plaintiffs' and the Patient Class Members' PHI, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the

sufficiency of its safeguards in place to control these risks; (c) designing and implementing inadequate cybersecurity safeguards and controls; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; (h) storing PHI and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff and the Class Members' PHI and medical records/information to a criminal third party.

278. But for WGH's wrongful breach of its duty of confidences owed to Plaintiffs and the Patient Class Members, their privacy, confidences, and PHI would not have been compromised.

279. As a direct and proximate result of WGH's breach of Plaintiffs and the Patient Class's confidences, Plaintiff and the Patient Class have suffered and/or are at a substantial increased risk of suffering injuries, including:

a. The erosion of the essential and confidential relationship between WGH – as a health care services provider – and Plaintiff and the Patient Class as patients;

b. Loss of the privacy and confidential nature of their PHI;

c. Theft of their PII and/or PHI;

d. Costs associated with the detection and prevention of identity theft or medical identity theft;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the WGH Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

i. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to WGH with the mutual understanding that WGH would safeguard Plaintiff's and the Patient Class Members' data against theft and not allow access and misuse of their data by others;

j. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in WGH's possession and is subject to further breaches so long as WGH fails to undertake appropriate and adequate measures to protect Plaintiff's and the Patient Class Members' data;

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by WGH; and

l. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PHI.

280. Additionally, WGH received payments from Plaintiffs and the Patient Class Members for services with the understanding that WGH would uphold its responsibilities to maintain the confidences of Plaintiffs' and Class Members' private medical information.

281. WGH breached the confidence of Plaintiffs and the Patient Class Members when it made an unauthorized release and disclosure of their confidential medical information and/or PHI and, accordingly, it would be inequitable for WGH to retain the benefit at Plaintiffs and Class Members' expense.

282. As a direct and proximate result of WGH's breach of its duty, Plaintiff and the Patient Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

Sixth Count
Unjust Enrichment
(On Behalf of Plaintiffs and The Classes)

283. Plaintiffs reallege and incorporate paragraphs 1-282 as if fully set forth herein. This count is pleaded in the alternative to the contract count above.

284. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including services rendered from and payments made by or on behalf of Plaintiffs and the Class Members.

285. As such, a portion of the value and monies derived from Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

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

287. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

288. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits 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 decision to prioritize its own profits over the requisite security.

289. 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 industry standards.

290. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

291. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

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

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

296. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they 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.

Seventh Count
Violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law
(On Behalf of Plaintiffs and the Patient Class)

297. Plaintiffs reallege and incorporate paragraphs 1-296 as if fully set forth herein.

298. Plaintiffs and the Patient Class purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

299. WGH engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii));

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or misunderstanding (73 Pa. Stat. Ann. § 201-2(4)(xi)).

300. WGH's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the Patient Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Patient Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and the Patient Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Patient Class Members' Private Information, including duties imposed by the FTC Act, LS U.S.C. § 5, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the Patient Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of

Plaintiffs' and the Patient Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

301. WGH's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

302. WGH intended to mislead Plaintiffs and the Patient Class Members and induce them to rely on WGH's misrepresentations and omissions.

303. Had Defendant disclosed to Plaintiffs and the Patient Class that WGH's data systems were not secure and, thus, vulnerable to attack, Plaintiffs and the Patient Class would not have used WGH's services and agreed to provide WGH with their Private Information and WGH would have been unable to continue in business. Instead, Defendant received, maintained, and compiled Plaintiffs and the Patient Class Members' Private Information as part of the services they provided without advising Plaintiffs and the Patient Class that WGH's data security practices were insufficient to maintain the safety and confidentiality of their Private Information. Accordingly, Plaintiffs and the Patient Class acted reasonably in relying on WGH's misrepresentations and omissions, the truth of which they could not have discovered.

304. Defendant acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiffs' and the Patient Class Members' rights.

305. As a direct and proximate result of WGH's unfair methods of competition and unfair or deceptive acts or practices and Plaintiffs' and the Patient Class Members' reliance on them, Plaintiffs and the Patient Class have suffered and will continue to suffer injury and actual harm in the form of, *inter alia*, (a) the compromise, publication, theft, and/or unauthorized use of

their Private Information; (b) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; (c) lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; (d) the continued risk to their Private Information, which remains in the possession of WGH and is subject to further breaches so long as WGH fails to undertake appropriate measures to protect Private Information in its possession; and (c) current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and the Patient Class.

306. Plaintiffs and the Patient Class seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

Eighth Count
Declaratory Judgment
(On Behalf of Plaintiffs and The Classes)

307. Plaintiffs reallege and incorporate paragraphs 1-306 as if fully set forth herein.

308. This 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.

309. An actual controversy has arisen in the wake of the Defendant's Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its

customers' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information.

310. Plaintiffs allege that Defendant's data security measures remain inadequate. Plaintiffs will continue to suffer injury because of the compromise of his Private Information and remain at imminent risk that further compromises of his Private Information will occur in the future.

311. 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 patients' Private Information and to timely notify patients of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various states' statutes; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure patients' Private Information.

312. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information.

313. 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 at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant 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.

314. 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 massive data breach occurs at Defendant, Plaintiffs and Class Members will likely be subjected to fraud, identify 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 pre-existing legal obligations to employ such measures.

315. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and the millions of individuals whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Classes;

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' Private 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 Private Information 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) Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Classes;

f) For an award of actual damages, nominal damages, compensatory damages, statutory damages, restitution or disgorgement, and/or punitive damages, in an amount to be determined, as allowable by law;

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

h) Pre- and post-judgment interest on any amounts awarded; and

i) 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: February 28, 2024

Respectfully submitted,

Benjamin F. Johns (Pa. Bar No. 201373)
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Phone: (610) 477-8380
bjohns@shublawyers.com

Andrew W. Ferich (Pa Bar No. 313696)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: (310) 474-9111

Fax: (310) 474-8585
aferich@ahdootwolfson.com

Danielle L. Perry*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
dperry@masonllp.com

Interim Co-Lead Class Counsel

Gary F. Lynch
Kelly Iverson
LYNCH CARPENTER, LLP
1133 Penn Ave., Fl. 5
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
kelly@lcllp.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
T: (865) 247-0047
gklinger@milberg.com

Kenneth J. Grunfeld
Jeff Ostrow
KOPELOWITIZ OSTROW P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
Tel: (215) 967-8799

Gary S. Graifman
KANTROWITZ GOLDHAMER & GRAIFMAN, P.C.
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
ggraifman@kgglaw.com

Kevin Laukaitis
LAUKAITIS LAW LLC

954 Avenida Ponce De León
Suite 205, #10518
San Juan, Puerto Rico 00907
klaukaitis@laukaitislaw.com

Attorneys for Plaintiffs and the Proposed Class

**pro hac vice*

IN THE PENNSYLVANIA COURT OF COMMON PLEAS
WARREN COUNTY

ROBERT PESSIA, PETER HETTMAN, HEIDI TULLER, and JEAN BERRY individually and on behalf of all others similarly situated, Plaintiffs, v. WARREN GENERAL HOSPITAL, Defendant.	CIVIL DIVISION CASE NO. 501 **CERTIFICATE OF SERVICE** CONSOLIDATED CLASS ACTION JURY TRIAL DEMANDED

I, Benjamin F. Johns, hereby certify that on February 28, 2024, I served a true and correct copy of the **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** upon defendant Warren General Hospital *via e- mail* to their counsel as follows:

Michael Riecken (mriecken@mullen.law)
Michael Jervis (mjervis@mullen.law)
MULLEN COUGHLIN
426 W. Lancaster Avenue
Suite 200
Devon, PA 19333

Benjamin F. Johns (PA Bar No. 201373)

EXHIBIT A

Patients' Rights

POLICY:

Warren General Hospital will provide healthcare services with an overriding concern for our patients' rights and dignity. State and federal laws guarantee certain rights to patients and their representatives, which are set forth the attached Statement of Patients' Rights.

PURPOSE:

To comply with state and federal laws that guarantee certain rights to patients and their representatives.

PROCEDURE:

The Statement of Patients' Rights is prominently displayed in all registration areas of the hospital and on the hospital website. In addition, the hospital provides the Statement of Patients' Rights to all inpatients and observation patients (or their representative) upon admittance, or as soon as possible thereafter.
The hospital will maintain documentation of receipt of the Statement of Patients' Rights in the patient's medical record.

References:

28 Pa. Code §103.22; 28 Pa. Code §101.163; 42 C.F.R. §482.13

Keywords:

Patients' Rights

Appendix A

STATEMENT OF THE PATIENT'S RIGHTS & RESPONSIBILITIES

As a patient, family member or guardian of a patient, we would like you to know that we are committed to delivering quality medical care that is effective and considerate. This document is a statement of our policy. We want you to know the rights you have under federal and Pennsylvania law as soon as possible in your hospital stay so that you may take an active role in your healthcare and can help us meet your needs.

As a **patient**, you have the right to receive care without discrimination due to age, sex, race color religion, sexual orientation, income, education, national origin, marital status, culture, language, disability, gender identity, physical disability or who will pay your bill. The physically disabled will have reasonable and equal access to the facilities, services, and programs of this hospital.

Patients will receive services and care that are medically suggested and within the hospital's services, its stated mission and required by law and regulation.

You have the right to:

- Respectful, considerate care given by skilled staff.
- Have your physician and a family member or other person of your choice promptly notified of your hospital admission.
- Know the names of the doctors and nurses, who provide your care, and the names and functions of other healthcare workers that care for you.
- Privacy concerning your own medical care. Case discussion, consultation, examination and treatment should be done in places designed to protect your privacy.
- Have all records pertaining to your medical care treated as confidential. If you request it, the hospital shall provide you access to your medical records unless restricted for medical or legal reasons. You will have access to your records within a reasonable time and for a reasonable fee.
- Know what hospital rules and regulations apply to your conduct as a patient.
- Expect emergency procedures to be implemented without unnecessary delay.
- Good quality care and high professional standards that are continually maintained and reviewed.
- Information about your current health, treatment, outcomes, recovery, ongoing healthcare needs and future health status in terms that you understand. This includes interpretation and translation, free of charge, in the language you prefer. This also includes providing you with help if you have vision, hearing or cognitive difficulties.
- Information upon discharge about your continuing healthcare requirements after discharge and the means for meeting them.
- Choose a support person, if needed, to act on your behalf to assert and protect your patient rights.

- Be involved in all aspects of your care and decisions about your care. When it is not medically advisable to give information to you, your information shall be given to your family member or other appropriate person. You have the right to information about alternative treatments and possible unexpected complications. You may be asked to sign your name before the start of a procedure and/or care. This is "informed consent," and it is not required in the case of an emergency.
- A proper assessment and management of pain, including the right to request or reject any or all options to relieve pain.
- Receive care in a safe setting.
- Be free of all forms of abuse or harassment.
- Receive care free from restraints or seclusion unless necessary to provide medical, surgical or behavioral health care.
- Decide to take part or not take part in research or clinical trials for your condition, or donor programs, that your doctor may suggest. Your participation in such programs is voluntary. You or your legal representative must give written permission before you participate. A decision not to take part in such programs will not affect your right to receive care.

You have the right to:

- Refuse any drugs, treatment, care or procedure offered by the hospital. You will be told of the medical consequences of your refusal. There may be times when care must be provided based on the law. You are responsible for your actions if you refuse care or do not follow care instructions.
- Request a consultation with another health care provider at your own expense.
- Receive a prompt and safe transfer to the care of others when Warren General is not able to meet your need or request for care or service. You have the right to know why a transfer might be required, as well as learning about other options for care. Warren General cannot transfer you to another hospital unless that hospital has agreed to accept you.
- Receive instructions on follow-up care and participate in decisions about your plan of care after you are out of the hospital.

YOU HAVE THE RIGHT TO RAISE A COMPLAINT OR GRIEVANCE

Being a good patient does not mean being a silent one. Tell hospital staff about your concerns or complaints regarding your care. This will not affect your future care.

Concerns, Complaints and Grievances during your hospital visit

Sometimes, a patient or family member may have a concern or complaint that can be quickly addressed during the hospital visit. We encourage you to contact the manager of the department or a member of your healthcare team so we can quickly address the concern.

Sometimes a more serious matter cannot be resolved quickly and while you are in the hospital. You may want to seek review of the quality of your care, coverage decisions and concerns about your discharge.

You may submit a complaint or grievance to the hospital in writing, by phone or in person. You may expect a timely response from the hospital in terms that you can understand. Alternatively, you may wish to submit your complaint or grievance to the PA Department of Health at the address and phone number below.

To share your concerns with the hospital, please contact the hospital's Patient Relations Department at:

Patient Relations Warren
General Hospital Two
Crescent Park West PO Box
68
Warren PA 16365
(814) 723-4973 extension 2087

You may submit your complaint or grievance to the Department of Health at: Pennsylvania Department of

Health
Acute & Ambulatory Care Services Health
& Welfare Building, Room 532 625 Forster
Street
Harrisburg PA 17180-0090
(800) 254-5164

YOUR RIGHT TO RECEIVE VISITORS

Warren General Hospital has an open visitation policy for most hospital units. This means that your family and friends may visit you at any time and may stay for as long as you wish them to stay. General visiting hours are 6:30 a.m. to 8:00 p.m. After 8:00 p.m., visitors must check in at the Emergency Care Center registration desk and receive an identification badge.

You have the right to:

- Decide if you want visitors while you are here. The hospital may need to limit visitors to better care for you or other patients.
- Choose the people who can visit you. These people do not need to be legally related to you. Tell your nursing team if you do not want certain visitors or if you do not want to receive visitors at certain times of the day.
- Designate a support person who may decide who can visit you if you become incapacitated.

We have special visiting hours on the following units:

- **Detoxification Services** -- Visitors must make an appointment with our staff. At that appointment, visitors will be given more information about the times of day and how often they may visit the patient, based upon the patient's needs.

- **Maternal Child Health** - The new mother makes the decision about who may visit and when.
- **Pediatrics** - Parents may visit at anytime. Visiting hours for all others are 1:00 p.m. until 8:00 p.m. and consent of the parent(s) is required.
- **Psychiatric Services** -- Visiting hours are 7:00 p.m. until 8:00 p.m. Alternate hours are available only with the approval of the psychiatrist or the nurse manager.
- **Surgical Services** - The patient may receive up to two visitors during pre-operative preparation and post-operative recovery.

Important Information for our Visitors:

We ask that visitors follow these rules:

- Please allow only 2 visitors at a time so as not to disrupt our other patients.
- Children under the age of 14 must be supervised by an adult.
- Visitors who are in the hospital overnight (between 8:00 p.m. and 6:30 a.m.) must wear a visitor badge. Ask your nursing team for a visitor badge.
- The hospital may limit or deny visits to individuals who have an infectious disease.
- Sometimes we require visitors to wear a mask or a gown before entering a patient room. These infection control precautions protect the patient, the visitor, and others.
- Visitors who are disruptive, violent, or too loud will be asked to leave.
- Visitation may be temporarily restricted when the patient's roommate needs rest or privacy.

YOUR RESPONSIBILITIES AS A PATIENT

The hospital desires to create a pleasant and safe environment during stay. Certain hospital rules are necessary to protect you and other patients. **We expect that you, your family, or caregiver will:**

- Provide accurate information about past illnesses, hospitalization, medication, advance healthcare directives, and other matters relating to your health.
- Report any condition that puts you at risk (for example, allergies.)
- Cooperate with all hospital staff and ask questions if you do not understand the instructions we give you or the procedures we describe.
- Be considerate of other patients, their families and visitors. Respect our visitation policies.
- Obey our no smoking policy, and do not consume alcoholic beverages.
- Tell us which of your family members or caregivers our healthcare team is authorized to discuss your medical care in the event you are unable to properly communicate with your healthcare team.
- During your hospital stay, you will only take medications that have been prescribed by your physician and administered by our healthcare team.
- Refrain from any illegal activity on hospital property. The hospital will report such activity to the police.

NOTICE OF PRIVACY PRACTICES

Your protected health care information is used or may be disclosed for purposes of treatment, payment, and operations to:

- Other health care professionals or providers for the purpose of providing you with quality health care. (Example: Another hospital, a nursing home, home health agency, or consults or referrals between physicians or reference laboratories.)
- Your insurance provider for the purpose of receiving payment for your needed health care services.
- Health care professionals for the purposes of ensuring we are providing quality health care services. (Example: Our quality assurance committee reviews patient records to monitor performance and quality.)
- Business associates who perform services such as billing, coding, consulting, transcription, and accounts receivable management.
- Training, certification, and licensing programs. (Example: Medical students and nursing students participate in training programs at WGH.)
- Customer service staff, medical or legal reviews, and auditors. (Example: Patients receive a questionnaire about the service they received and these are used to improve our service to you.)
  Public health or law enforcement when the law requires it.
  State or federal agencies for purposes of health care cost containment, determining medical necessity, or appropriateness of services.
  Report a defective device or problematic event regarding a biological product (food or medication). (Example: The FDA requires reporting of defective equipment).
- Send you appointment reminders, treatment alternatives, or information regarding other health related benefits and services.
- Visitors, callers, clergy, and room deliveries, if you agree to be in our hospital directory and these people ask for you by name.
- Other situations where Warren General Hospital may use or disclose your protected health information include: organ and tissue donations, workers compensation, coroners, medical examiners, and funeral directors.

You have the right to:

- Receive a copy of this Privacy Notice.
- Request a restriction of the use of your health care information unless the restriction conflicts with providing you health care or in the event of an emergency. The Hospital will review each restriction request, but reserves the right to deny any restriction request received.
- Make reasonable requests to receive communications about your health care at an alternate address or by means other than by mail.
- Make a written request to review and/or photocopy your health care information (Copies may be subject to reasonable charges.)

- Request changes to your health care information. These requests must be made in writing.
- Know who has received your health care information for purposes other than treatment, payment, and operations of the hospital, and for what purpose, with some exceptions as defined by law.

If you believe your rights to privacy have been violated, you may file a complaint with our privacy officer or notify the Department of Health and Human Services. All complaints will be investigated. No action will be taken against you for filing a complaint with the hospital. **You may mail a complaint to:**

Attn: Privacy Officer
Warren General Hospital
Two Crescent Park West, PO Box 68
Warren PA16365

Normally, we will require your signed authorization before disclosing your medical information outside the hospital, unless it is required by law. You may revoke your permission to release confidential information at any time. The hospital abides by the terms of this notice. The hospital may make changes to the Privacy Notice. Changes will be effective for all protected health information kept by the hospital. The revised Privacy Notice will be available at the point of service.
Notice Effective: May 18, 2012

AD VANCE HEALTHCARE DIRECTIVES

You have the right to create advance medical directives, which are legal papers that allow you to decide now what you want to happen if you are no longer able to make your own decisions about your care. You have the right to appoint someone to make healthcare decisions on your behalf. You have the right to have hospital staff comply with these directives. You are not required to have an advance directive in order to receive care and treatment in this facility.

What are advance healthcare directives? There are two common types:

- **Living Will.** This document tells your healthcare team what types of treatment you will want or not want when you get to the end of your life. A Living Will is only used when you have a non- curable, terminal illness **and** you are unable to communicate with your healthcare team. If you are not sure what type of end-of-life treatment you may want, you can use the Living Will to designate a person to make those decisions for you, when the time comes.
- **Power of Attorney.** A Power of Attorney lets you name another person to make healthcare decisions for you. You decide what powers you want to give another person and when those powers will take effect. Since a Living Will is only effective for end-of-life situations, a Power of Attorney is useful when you cannot communicate for other reasons.

What should I do with my advance healthcare directive? You should give a copy to your family doctor, to the hospital, your family, and those people you have named to help make decisions for you if you cannot.

Can I change my advance healthcare directive? You can change your mind and revoke a Living Will or Power of Attorney at any time. To do this you need to tell your family or healthcare team that you revoke the document. Another way to revoke your advance healthcare is to make a new one, sign it and date it.

What if I don't have an advance healthcare directive? As long as you are able to communicate with your physician, you will decide what type of healthcare you want or do not want. If you are unable to communicate with your physician, your physician will discuss this with your family. If you have no family, a court order may be necessary to decide what type of treatment is best for you.

Where can I get forms to complete an advanced healthcare directive? Ask your physician, nurse, or social worker for the forms to make an advance healthcare directive.

HOSPITAL BILLS

You are responsible to promptly pay for the healthcare that you receive, whether through your insurance or through your own funds. Some services may not be covered by insurance. Some services may have a patient copayment or deductible. If you think you may need financial assistance with your bill, please contact our financial counselor at (814) 723-4973 extension 1325.

Tell us when your name, address, telephone number, or insurance information changes during your hospitalization or soon after you received services from our hospital.

You have the right to:

- Request, examine and receive a detailed explanation of your hospital bill.
- Receive information and counseling on ways to help pay for your hospital bill.

HEALTHCARE PAYMENT ASSISTANCE PROGRAM

If you do not have healthcare insurance or have limited funds, you may be eligible for our healthcare payment assistance program. Discounted or free care is based upon income and household size. A hospital representative will review and verify the financial information you provided during the application process. We reserve the right to ask you to receive a denial from Medical Assistance if you may meet benefit criteria. **If you would like more information about this program, please contact our Patient Accounts Department at (814) 723-4973 extension 1325.**

Patient Care Policy 101.03 - Appendix B Effective 10-20-2014

PATIENT'S CIVIL RIGHTS

a. Inpatient and outpatient care including all clinic locations, emergency room care and any contracted services for patients shall be provided without regard to race, color, national origin, sex, sexual preference, religion, ancestry, age, handicap or disability.

b. All patients shall be assigned to rooms, floors and sections in accordance with their medical needs.

c. Patients shall not be asked whether they are willing or desire to share a room with a person of another race, religion, sexual preference, ancestry, age, handicap or disability.

d. Employees shall be assigned to patient services without regard to the race, color, national

origin, religion, sex, sexual preference, religion, ancestry, age, handicap or disability of either the patient or employee.

e. Transfer of patients from rooms assigned or selected, or both, shall not be made for other than valid medical reasons.

f. At discharge, patients shall be referred only to those skilled nursing care facilities, intermediate care facilities, personal care facilities or foster homes which are not known to the hospital to be in noncompliance with the provisions of the Pennsylvania Human Relations Act (43 P.S. §§ 951-963). The hospital shall report immediately to the Compliance Office of the Department of Health all instances of post-hospital discriminatory practices experienced by patients referred by the hospital when such practices are brought to the attention of the hospital.

g. All training programs and opportunities offered by the hospital shall be open to qualified applicants without regard to race, creed, color, national origin, sex, sexual preference, religion, ancestry, age, handicap or disability; and recruitment efforts for these shall include sources having potential racial minority applicants.

Revision #: 8

Approval Signatures

Step Description	Approver	Date