UNITED STATES DISTRICT
IN THE SOUTHERN DISTRICT COURT OF IOWA
CENTRAL DIVISION

JANE DOE, Individually and on behalf of all others Similarly situated,	)	
Plaintiff,	)	
v.	)	Case No.: 4:18-cv-453
IOWA HEALTH SYSTEM, doing business As UNITY POINT HEALTH, an Iowa non-profit corporation.	)	**CLASS ACTION PETITION**
Defendant.	)	

CLASS ACTION COMPLAINT

COMES NOW Plaintiff, Jane Doe[1], on behalf of herself and as a representative of all similarly situated, submits the following Petition against Defendant Iowa Health System, doing business as UnityPoint Health ("UnityPoint" or "Defendant") to, without limitation, obtain actual and punitive damages, restitution, and obtain a declaration that Defendant's actions were unlawful as further set forth below. Plaintiff alleges the following:

PARTIES

1. Plaintiff Jane Doe is a resident and citizen of the state of Iowa, residing in Davenport, Iowa.

2. Defendant Iowa Health System is a non-profit corporation organized and existing under the laws of the State of Iowa with its principal place of business located 1776 West Lakes Parkway, Suite 400, West Des Moines, Iowa 50266. Defendant transacts business throughout the states of Iowa, Wisconsin and Illinois. Defendant is doing business as UnityPoint Health. At all

[1] Due to the highly private nature of the case and allegation of the Petition, Plaintiff requests that her identity be kept confidential. Plaintiff therefore intends to file a motion to proceed under pseudonym.

times material to this action, acting alone or in concert with others, UnityPoint has advertised, marketed, distributed, and sold its health care services to patients and consumers in the states of Iowa, Wisconsin and Illinois.

NATURE OF THE ACTION

3. On or about November 1, 2017, Defendant UnityPoint is a multi-hospital delivery and health care system serving parts of Wisconsin, Iowa, and Illinois. UnityPoint's database containing Plaintiff protected health information was breached. UnityPoint reportedly discovered the 2017 breach between February 7, 2018 and February 15, 2018.

4. On or about April 17, 2018, Plaintiff received a form letter notifying her that Plaintiff's confidential medical records and information were disclosed in the breach. The letter informed Plaintiff that UnityPoint wanted to make Plaintiff aware of the situation and suggested certain practices "as a general matter" that individuals can follow to help protect themselves against medical identity theft. The notification letter did not mention whether Defendant would take any steps to remediate the harm from the data breach, including whether it would offer protective services such as credit monitoring, identity theft protection, or "dark web" searches.

5. On or about May 31, 2018, Defendant discovered a second breach of its patient database containing confidential patient medical records and information. It appears that the second breach began on or about May 14, 2018.

6. On or about August 2, 2018, Plaintiff received a form letter notifying them that the 2018 breach which resulted in unauthorized access of confidential patient medical records and information.

7. The August 2, 2018 letter informed Plaintiff that UnityPoint wanted to make Plaintiff aware of the 2018 breach and what the victims could do to protect themselves against medical identity theft by "monitoring [their] health information." The notification letter further

stated,

> "To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft." [**Emphasis in original**.]

8. Plaintiff, and the patients and consumers she seeks to represent, are victims of Defendant's negligence and unfair practices who have suffered tangible and concrete injury-in-fact. Accordingly, Plaintiff, individually, and on behalf of a class of similarly situated individuals (the "Class" or "Class Members" as further defined below), bring this lawsuit and seek compensatory damages, punitive damages, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in the possession of Defendant.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this action under 28 U.S.C. §1332(d) of the Class Action Fairness Act because the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are at least 100 members of the proposed Class, and at least one member of the proposed Class is a citizen of a different state from the Defendant.

10. Pursuant to 28 U.S.C. § 1367 this Court has supplemental jurisdiction over the state statutory and common law claims alleged herein.

11. This Court has personal jurisdiction over Defendant as Defendant is a resident of the State of Iowa.

12. Venue is appropriate in this district under 28 U.S.C. §1391 because Defendant resides in this District.

COMMON FACTUAL ALLEGATIONS

13. Defendant UnityPoint (previously known as Iowa Health System) is a network of hospitals, clinics, home care services, and health insurers in Iowa, Wisconsin and Illinois.

Defendant's health system now encompasses eight metropolitan areas in three states.

14. At least as early as the period between February 7, 2018 and February 15, 2018, UnityPoint discovered that at least 16,429 patients' and consumers' personal and protected health information, including patient names, birth dates, diagnosis codes, addresses, private mobile and landline phone numbers, email addresses, medical record numbers, treatment information, diagnoses, lab results, medications, providers, dates of service, insurance information, policy numbers, Medicare numbers, billing information, other financial information, and Social Security numbers (the "Personal Health Information" or "PHI"), had been accessed through one or more employees' email account(s) in connection with the 2017 breach.

15. The medical records disclosed by Defendant in the 2017 and 2018 breaches contained highly sensitive medical information including drug and alcohol information, mental health information, and patients who suffer from sexually transmitted diseases.

16. Once the private information about Plaintiff's medical conditions are disclosed, the information explodes beyond the control of Defendant and spreads like wildfire throughout the general public.

17. Plaintiff immediately faced the anxiety, embarrassment, shame, concern, and stigma of knowing that the confidentiality of their medical information has been destroyed.

18. Defendant is required to maintain the strictest privacy and confidentiality of patient medical records.

19. On or about May 31, 2018, UnityPoint discovered that 1.4 million patients' and consumers' PHI and other personal information, had again been accessed through one or more employees' email account(s) in connection with the 2018 breach. The 2018 breach disclosed confidential medical information from as far back as March 14, 2018. Defendant claims the 2018 breach went undetected for several months.

The 2017 Disclosure of Confidential Medical Information

20. UnityPoint ultimately admitted the 2017 breach to its patients, consumers, and the public on or about April 16, 2018. In a notification form letter from RaeAnn Isaacson, Privacy Officer for UnityPoint to Plaintiff and Class Members dated April 16, 2018 (the "First Notice Letter" or "First Letter"), UnityPoint admitted it had,

> "discovered your protected health information was contained in an impacted email account, including your name and one or more of the following: date of birth, medical record number, treatment information, surgical diagnosis, lab results, medication(s), provider(s), date(s) of service and/or insurance information."

21. In an effort to minimize the harm, UnityPoint did not disclose all the known facts about the 2017 breach in the First Notice Letter when it falsely claimed, "The information did not include your Social Security number."

22. The First Notice Letter further admitted that, "[w]e want to make impacted individuals aware of the situation so they can take precautionary measures to protect their health information." The First Notice Letter then further falsely claimed UnityPoint had no information indicating that the stolen medical information "will be used for any unintended purposes." Defendant's Letterthen listed some practices "[a]s a general matter" that individuals can take to protect themselves from medical identity theft, including:

> "Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
>
> - Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement for copies of medical records from the date of the potential access (noted above) to current date.
> - Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize."

23. The First Notice Letter did not mention whether Defendant would take any steps to remediate the 2017 disclosure, or whether it would offer any assistance to its patients to mitigate the harm they suffered. The First Notice Letter did not mention whether Defendant had notified law enforcement or the Federal Trade Commission of the First Data Breach. The First Notice Letter neither referred victims to any website for assistance (such as the Federal Trade Commission's identity theft website), nor suggested Plaintiff and the Class Members consider any of the following precautions: notifying local law enforcement; giving the Plaintiff assurances that Defendant took steps to regain the stolen information from the person or persons to whom the information was disclosed; obtaining protection through monitoring of the dark web; getting a free copy of their credit report; monitoring their credit for signs of identity theft; placing a fraud alert on their credit report; requesting a credit freeze; notifying their insurance companies, health providers, and financial institutions; requesting their insurance companies, health providers, and financial institutions notify them of possible instances of identity theft; requesting new account numbers; or closing accounts. The First Notice Letter did not describe any steps Defendant is taking to investigate the 2017 disclosure, protect against future breaches, or remediate or mitigate the harm from the 2017 disclosure such as searching for and locating the Plaintiff's medical information.

24. Nowhere did Defendant describe any steps it is taking to protect against future breaches, or remediate and mitigate the harm from the 2017 disclosure.

25. Despite failing to take any steps to mitigate harm to the entire group of patients who medical information was disclosed, Defendant purchased some form of limited credit monitoring services for up to a year for a small portion of Class Members affiliated with Defendant.

26. Plaintiff and other Class Members have suffered injury that can be directly traceable to Defendant from the disclosure of confidential medical information and other personal

information acquired in the 2017 breach, including without limitation lost medical expenses, lost benefit of the bargain, lost services, overpayment for privacy services which Plaintiff did not receive, fraud in the inducement wherein Plaintiff would not have obtained treatment from Defendant knowing that their medical information was not safe and protected, loss of enjoyment of life, Plaintiff paying more for privacy services which they did not receive, embarrassment, humiliation, and emotional distress.

27. The 2017 disclosure is not the first evidence of UnityPoint's failure to secure confidential medical information. On May 11, 2016, a UnityPoint Health Affiliated Covered Entity healthcare provider in Iowa notified the U.S. Dept. of Health and Human Services Office for Civil Rights (the "HHS") of an unauthorized access/disclosure of electronic medical records affecting 1,620 individuals. Additionally, UnityPoint affiliated healthcare provider UW Health notified the HHS on May 25, 2017 of an email hacking/IT incident affecting 2,036 individuals.

28. Rather than taking steps to fairly and fully inform Plaintiff and the Class Members about the true facts regarding the First Data Breach and take its own "precautionary measures" to mitigate and remediate at its cost the injury to affected patients, Defendant instead misrepresented the nature, breadth, scope, harm, and cost of the 2017 disclosure to Plaintiff and the Class Members when it falsely stated in the Notice Letter that, "The [stolen] information did not include your Social Security number", and "[w]e have no information to date indicating that your Protected Health Information (PHI) involved in this incident was or will be used for any unintended purposes."

29. Defendant knew, or should have known, when it sent the First Notice Letter that the stolen information did include affected patient Social Security numbers. Defendant further knew, or should have known, it possessed information that makes it highly likely the confidential medical information will be used for an unintended purpose. Defendant knowingly, intentionally, and recklessly made these false statements in an effort to conceal and minimize the harm and injury

to Plaintiff and the Class Members caused by the 2017 disclosure, and to induce them and the public to continue to use, and to expand the use of, Defendant's services.

The 2018 Disclosure of Confidential Medical Information

30. UnityPoint informed its patients of another disclosure of confidential medical information on or about July 30, 2018. In a notification form letter to Plaintiff and Class Members, again signed by RaeAnn Isaacson, Privacy Officer for UnityPoint dated July 30, 2018 (the "Second Notice Letter" or "Second Letter"), UnityPoint admitted that confidential medical information was wrongfully disclosed. The information disclosed included patients' name, address, date of birth, Social Security number, driver's license number, medical record number, medical information, treatment information, surgical information, diagnosis, lab results, medication(s), provider(s), date(s) of service and/or insurance information.

31. Defendant falsely informed patients that its electronic medical systems were not impacted by the 2018 disclosure.

32. Plaintiff and other Class Members have suffered injury that can be directly traceable to Defendant from the disclosure of confidential medical information and other personal information acquired in the 2018 breach, including without limitation lost medical expenses, lost benefit of the bargain, lost services, overpayment for privacy services which Plaintiff did not receive, fraud in the inducement wherein Plaintiff would not have obtained treatment from Defendant knowing that their medical information was not safe and protected, loss of enjoyment of life, Plaintiff paying more for privacy services which they did not receive, embarrassment, humiliation, and emotional distress.

33. The value of Plaintiff's and the Class Members' medical information on the black market is considerable. Stolen medical information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web"

Internet websites, making the information publicly available, for a substantial fee of course.

34. Defendant has disclosed and given access to the confidential medical records and information of Plaintiff and the Class Members for criminals to use in the conduct of criminal activity.

35. Defendant is required by law to protect patient medical records and information by having the most up to date computer systems.

36. Each time Plaintiff and the Class Members received treatment from Defendant they were given a notice that their medical information would be protected and would not be disclosed without written authorization from the patient.

CLASS ACTION ALLEGATIONS

37. Plaintiff brings this action pursuant to pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of herself and all Members of the Class and Subclasses defined as:

> Patients and customers of UnityPoint whose medical information was released as a result of the unauthorized disclosure of their medical records and information on or about November 1, 2017 and May 14, 2018.

38. The Excluded from the Class are Defendants, any affiliate, parent, employee or subsidiary of Defendants; any officer, director, or employee of Defendants; anyone employed by counsel for Plaintiff in this action; and any Judge to whom this case is assigned as well as his or her immediate family.

39. This action has been brought and may be properly maintained as a class action under FRCP 23.

40. **Numerosity of the Class – Rule 23(a)(1).** Class members are so numerous that their individual joinder is impracticable. The precise number of Class members and their addresses can be obtained from information and records in Defendants' possession and control. Class

members may be notified of the pendency of this action by mail or by published notice or other appropriate methods.

41. **Existence and Predominance of Common Questions of Law and Fact – Rule 23(a)(2).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual Class members. These common legal and factual questions, each of which may also be certified under FRCP 23, include the following:

a. Whether Defendant breached its fiduciary duties to Plaintiff and the Class;

b. Whether Defendant breached its contract with Plaintiff and the Class;

c. Whether Defendant invaded Plaintiff's and the Class' privacy;

d. Whether Defendant acted negligently with respect to Plaintiff and the Class;

e. Whether Plaintiff and the other Class members are entitled to equitable relief, including declaratory relief, restitution, rescission, a preliminary and/or a permanent injunction;

f. Whether Plaintiff and the other Class members are entitled to damages, including punitive damages, and/or other monetary relief; and

g. Whether this case may be maintained as a class action under FRCP 23.

42. **Typicality – Rule 23(a)(3).** Plaintiff's claims are typical of the claims of the Class because she was a patient of Defendant, and his personal information was compromised in the 2017 and 2018 breaches. Moreover, Plaintiff and the Class sustained similar injuries as a result of Defendant's uniform conduct and their legal claims all arise from the same policies and practices of Defendant.

43. **Adequacy of Representation – Rule 23(a)(4).** Plaintiff will fairly and adequately protect the interests of Class members. Plaintiff has retained counsel competent and experienced

in complex class action litigation, and Plaintiff will prosecute this action vigorously. Plaintiff has no interests adverse or antagonistic to those of the Class.

44. **Superiority – Rule 23(b).** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are small compared with the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

45. In the alternative, the Class may be certified under Rule 23(b)(1) and/or (b)(2) because:

a. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudication with respect to individual Class members that would establish incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class members not parties to the

adjudications, or substantially impair or impede their ability to protect their interests; and/or

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final and injunctive relief with respect to the Class members as a whole.

COUNT I – INVASION OF PRIVACY
(On Behalf of the Plaintiff and Class for Invasion of Privacy)

46. Plaintiff incorporates by reference and re-alleges all paragraphs previously alleged herein. Plaintiff asserts this cause of action on behalf of the Class against Defendant.

47. At all times relevant hereto, Defendant, as a result of its provider-patient relationship with its patients -- Plaintiff and the Class Members -- had the duty to keep Plaintiff's medical information private.

48. Defendant breached its duty to Plaintiff and the Class Members by intentionally disclosing highly sensitive and confidential medical information to the public without obtaining authorization from Plaintiff.

49. Defendant breached its duty to keep Plaintiff's medical information private by publicizing matters of a highly sensitive nature to the public concerning the private life and medical information of Plaintiff.

50. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's confidential medical information, Plaintiff and the Class suffered damages including, without limitation, lost medical expenses, lost benefit of the bargain, lost services, overpayment for privacy services which Plaintiff did not receive, fraud in the inducement wherein Plaintiff would not have obtained treatment from Defendant knowing that their medical information was not safe and protected, loss of enjoyment of life, Plaintiff paying more for privacy services which they did not receive, embarrassment, humiliation, and emotional distress.

COUNT II – NEGLIGENT TRAINING AND SUPERVISION
(On behalf of Plaintiff and the Class for Negligent Training and Supervision)

51. Plaintiff incorporates by reference and re-alleges all paragraphs previously alleged herein. Plaintiff asserts this cause of action on behalf of the Class against Defendant.

52. At all times relevant hereto, Defendant owed a duty to Plaintiff and the Class to train and supervise competent employees and agents regarding its duties of privacy and confidentiality owed to its patients.

53. Defendant breached its duty to Plaintiff and the Class by allowing its employees, agents, or representatives to disclose confidential medical information to the public.

54. As a direct result of Defendant's negligent training and supervision, Plaintiff and the Class suffered damages, including, without limitation, lost medical expenses, lost benefit of the bargain, lost services, overpayment for privacy services which Plaintiff did not receive, fraud in the inducement wherein Plaintiff would not have obtained treatment from Defendant knowing that their medical information was not safe and protected, loss of enjoyment of life, Plaintiff paying more for privacy services which they did not receive, embarrassment, humiliation, and emotional distress.

COUNT III – BREACH OF FIDUCIARY DUTY
(On Behalf of the Plaintiff and Class for Breach of Fiduciary Duty)

55. Plaintiff incorporates by reference and re-alleges all paragraphs previously alleged herein. Plaintiff asserts this cause of action on behalf of the Class against Defendant.

56. Defendant has a fiduciary duty of confidentiality to its patients.

57. Defendant breached its duty to Plaintiff and the Class by disclosing its customers' confidential medical information to third parties without consent or authorization.

58. As a direct result of Defendant's breach of its fiduciary duty, Plaintiff and the Class have suffered damages, including, without limitation, lost medical expenses, lost benefit of the

bargain, lost services, overpayment for privacy services which Plaintiff did not receive, fraud in the inducement wherein Plaintiff would not have obtained treatment from Defendant knowing that their medical information was not safe and protected, loss of enjoyment of life, Plaintiff paying more for privacy services which they did not receive, embarrassment, humiliation, and emotional distress.

COUNT IV – NEGLIGENCE
(On behalf of Plaintiff and the Class for Negligence)

59. Plaintiff incorporates by reference and re-alleges all paragraphs previously alleged herein. Plaintiff asserts this cause of action on behalf of the Class against Defendant.

60. Defendant owed Plaintiff and the Class a duty to exercise the highest degree of care in safeguarding and protecting the medical information of its patients. This duty included securing medical records and information and implementing policies regarding properly securing and protecting medical records and information of Plaintiff and the Class from unauthorized disclosure.

61. Defendant further owed Plaintiff and the Class a duty to notify them within a reasonable time frame of any breach to the security of their PHI under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320(d), *et seq*. ("HIPAA") and other state and federal laws referenced herein. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and the other Class Members the scope, nature, and occurrence of the Data Breaches. This duty is required and necessary in order for Plaintiffs and the Class to take appropriate measures to protect their PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breaches.

62. Defendant breached its duty to exercise reasonable care in protecting the personal information of Plaintiff and the Class by (1) failing to implement security measures to protect the information of Plaintiff and the Class; (2) failing to implement policies regarding the security of

medical records and information; and (3) failing to implement security measures such as properly securing medical records.

63. As a result of Defendant's negligence, Plaintiff and the Class suffered damages including without limitation the lost medical expenses, lost benefit of the bargain, lost services, overpayment for privacy services which Plaintiff did not receive, fraud in the inducement wherein Plaintiff would not have obtained treatment from Defendant knowing that their medical information was not safe and protected, loss of enjoyment of life, Plaintiff paying more for privacy services which they did not receive, embarrassment, humiliation, and emotional distress.

COUNT V – BREACH OF CONTRACT
(On behalf of Plaintiff and the Class for Breach of Contract)

64. Plaintiff incorporates by reference and re-alleges all paragraphs previously alleged herein. Plaintiff asserts this cause of action on behalf of the Class against Defendant.

65. In Defendant's Notice of Privacy Practices, it states:

> "USES AND DISCLOSURES REQUIRING YOUR AUTHORIZATION. There are many uses and disclosures we will make only with your written authorization. These include: • Uses and Disclosures Not Described Above. We will obtain your authorization for uses and disclosures of your health information that are not described in the Notice above.
>
> NOTICE IN THE CASE OF BREACH. You have the right to receive notice of an access, acquisition, use or disclosure of your health information that is not permitted by HIPAA, if such access, acquisition, use or disclosure compromises the security or privacy of your PHI (we refer to this as a breach). We will provide such notice to you without unreasonable delay but in no case later than 60 days after we discover the breach.
>
> WHO WILL FOLLOW THESE PRIVACY PRACTICES? The health care organizations that are a part of UnityPoint Health have collectively formed an Affiliated Covered Entity or "ACE" under the HIPAA regulations for purposes of HIPAA compliance. A full list of organizations in the UnityPoint Health ACE, called "Affiliates" are listed in Appendix A to this Notice. Our rules to protect your privacy will be followed by all workforce members of the site where you are being treated, as well as physicians and other health care practitioners

> with permission to provide services at our sites who are independent of any UnityPoint Health Affiliate (together called "the UnityPoint Health ACE" in this Notice).
>
> WHAT HEALTH INFORMATION IS COVERED UNDER THIS NOTICE? This Notice covers health information at the UnityPoint Health ACE that may be written (such as a hard copy medical record file), spoken (such as physicians discussing treatment options), or electronic (such as billing records kept on a computer).
>
> **Information Security**
>
> We will use security procedures to protect personal information you submit to us from misuse or unauthorized disclosure. The personal information that you submit to us is stored in a secure database behind an electronic firewall. You can access your personal information only by using a password. We encourage you to change your password regularly and not to share it with anyone.
>
> Access to the data is limited to a few computer technicians for our site who need to maintain the database and who also use passwords for that access, as well as outside vendors who may occasionally assist us in maintaining and improving our hardware and software tools.
>
> **Patient Privacy at UnityPoint Health**
>
> Protecting the privacy of our patients' information is a key part of our goal to provide the best outcome for every patient every time. Across the United States, the privacy of patients' health information is protected by a federal law and regulations (commonly referred to as "HIPAA") that establish minimum standards for maintaining the privacy and security of patients' information. In addition, the states where we treat our patients also have state laws that provide additional protections for certain types of health information. At UnityPoint Health, we have a compliance program that includes policies implementing patient privacy and security requirements mandated under federal and state law. We provide training to our employees on the importance of complying with these policies and regularly conduct audits to confirm the effectiveness of our privacy and security compliance policies."

66. Defendant's notice constitutes an agreement between Defendant and its patients.

67. These representations go beyond what Defendant is already obligated to do under applicable laws.

68. Defendant breached its agreement with Plaintiff and the Class by (1) failing to implement security measures to fulfill their agreement with their patients, and (2) failing to implement security measures such as securing medical records and information.

69. Plaintiff and the Class have been damaged by Defendant's breach of their obligations because their personal and medical information has been compromised and the loss of costs paid to Defendants for the maintenance of the confidentiality of medical information.

70. It was a violation of UnityPoint's privacy covenants, warranties, and promises to disclose Plaintiff's and Class Members' highly confidential medical records and information in the manner described above. As a result of Defendant's breach of contract, Plaintiff and Class Members did not receive the full benefit of their bargain and instead received services that were less valuable than described in their contracts.

71. As part of the contract between Defendant and Plaintiff and the Class Members, Defendant offered to provide health care and health care related services in exchange for their business and payments from Plaintiff and the Class Members or their insurers on their behalf, Defendant promised: (a) "[We] will protect your medical records and privacy"; (b) that their rules to protect Plaintiff and the Class Members' privacy will be followed by all workforce members of the site where they are being treated; (c) it will use security procedures to protect personal information which Plaintiff and the Class Members submit to it from misuse or unauthorized disclosure; (d) that the personal information that Plaintiff and the Class Members submit to it is stored in a secure database behind an electronic firewall; (e) that access to medical records and information is limited to a few computer technicians as well as outside vendors who may occasionally assist it in maintaining and improving our hardware and software tools; and (f) that it has a compliance program that includes policies implementing patient privacy and security requirements mandated under federal and state law.

72. UnityPoint also agreed to provide its health care services in a professional manner and only to share it with authorized employees as part of their work to support patient care.

73. Plaintiff and Class Members accepted UnityPoint's offer and went to, and paid, Defendant for their health care services. Plaintiff and the Class Members contracted for and expected to receive the privacy benefits in accordance with the terms and warranties set forth above. Defendant breached the privacy obligations under its contract as set forth above and Plaintiff and the Class Members have been injured and damaged as a result thereof.

74. Plaintiff and the other Class Members performed their obligations under the agreements. Defendant violated the terms of the contract by disclosing and allowing unauthorized access to Plaintiff's and the other Class Members' confidential medical records and information for unauthorized purposes without first obtaining Plaintiff's or the other Class Members' consent, or encrypting or otherwise protecting the information in a form which could not reasonably be used to identify them.

75. Defendant breached its contracts with Plaintiff and Class Members by failing to reasonably safeguard its systems and health information from the breaches. Defendant violated the terms of the contract by failing to take appropriate measures to protect Plaintiff's and the other Class Members' personal information in accordance with its promises and representations. Defendant violated the agreement by failing to comply with applicable laws regarding the access, correction, and/or deletion of confidential medical records and information, and notification to affected persons.

76. Plaintiff and Class Members have been injured as a result of Defendant's breach of contract and are entitled to damages.

77. As a result of Defendant's unlawful misconduct and breach of its contract with Plaintiff and the Class Members, Plaintiff and the Class Members have suffered additional

pecuniary loss and injury-in-fact, including without limitation the improper disclosure of their confidential medical records and information, lost benefit of their bargain, lost value of their confidential health information, attorney fees and costs.

COUNT VI
(Private Right of Action for Iowa Consumer Frauds Act, Iowa Code § 714H, *et seq*. On Behalf of Plaintiff and the Class)

78. Plaintiff and the Class Members and incorporate the above allegations as if fully set forth herein.

79. The Iowa Private Right of Action for Consumer Frauds Act prohibits unfair and deceptive trade practices in the sale, lease, or advertisement of a product or service, and in the solicitation of charitable contributions. The Iowa Private Right of Action for Consumer Frauds Act's purpose is to protect consumers against these unfair and deceptive business practices and provide efficient and economical procedures to secure such protection.

80. Defendant operating in Iowa has violated the Act by engaging in the unfair and/or deceptive acts and practices described herein, which were and are intended to and did and do result in the purchase of Defendant's products and services by consumers, including Plaintiff and the Class Members.

81. As a result of Defendant's unfair and deceptive business practices, Plaintiff and the Class Members have lost money or property and therefore seek their actual damages. Plaintiff and the Class Members also seek and are entitled to an order enjoining Defendant from continuing to engage in the unfair and deceptive business practices alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests the Court:

1. For an order certifying the proposed Class, and appointing Plaintiff by and through his counsel of record to represent the proposed Class;

2. For an order declaring that Unity Point has violated its fiduciary duties to Plaintiff and the Class.

3. For an Order declaring that Unity Point has breached its contract of confidentiality with Plaintiff and the Class.

4. For an Order that Unity Point's actions were outrageous so as to cause Plaintiff and the Class damages.

5. For an Order declaring that Unity Point has acted negligently so as to cause Plaintiff and the Class damages.

6. For an order awarding Plaintiff and Class members damages in an amount to be proven at trial, including punitive damages, together with pre-trial and post-trial interest thereon;

7. For an order awarding Plaintiff and Class members restitution, disgorgement, or other equitable relief as the Court deems proper, including corrective notice;

8. For an order enjoining Unity Point from continuing to engage in the unlawful business practices alleged herein;

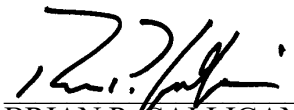
9. For an order awarding Plaintiff and the Class reasonable attorneys' fees and costs of suit, including expert witness fees; and

10. For an order awarding such other and further relief as this Court deems just and proper.

JURY DEMAND

Plaintiff hereby demand a trial by jury on all issues so triable.

Respectfully submitted,



BRIAN P. GALLIGAN AT0002632
GALLIGAN LAW P.C.
The Plaza - Suite 5
300 Walnut Street
Des Moines, Iowa, 50309-2239
Telephone: (515) 282-3333
Facsimile: (515) 282-0318
Email: bgalligan@galliganlaw.com

ATTORNEY FOR PLAINTIFFS

Pro Hac Vice pending:

Maureen M. Brady MO# 57800
Lucy McShane MO# 57957
McSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Phone: (816) 888-8010
Fax: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com

-and-

Anne Schiavone MO#49349
Brandon Corl MO# 58725
Wade A. Schilling MO#67235
HOLMAN SHIAVONE, LLC
4600 Madison, Ste. 810
Kansas City, MO 64111
Telephone (816) 283-8738
Facsimile (816) 283-8739
Email: aschiavone@hslawllc.com

ATTORNEY FOR PLAINTIFFS
(Pro Hac Vice Pending)