

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

YVONNE MART FOX, individually and
on behalf of all others similarly situated,

Plaintiff,

v.

IOWA HEALTH SYSTEM, INC., doing
business as UNITYPOINT HEALTH, an
Iowa non-profit corporation,

Defendant.

Case No.: 18-cv-327

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff YVONNE MART FOX ("Fox" or "Plaintiff"), individually and on behalf of all other persons similarly situated, by her undersigned attorney, files this Class Action Complaint against IOWA HEALTH SYSTEM, INC., doing business as UnityPoint Health ("UnityPoint" or "Defendant") to, without limitation, obtain damages, injunctive relief, restitution, and obtain a declaration that Defendant's actions were unlawful as further set forth below. Plaintiff alleges the following based upon personal knowledge as to herself and her own acts, and on information and belief as to all other matters, including, *inter alia*, investigation conducted by and through her attorney.

NATURE OF THE ACTION

1. Defendant UnityPoint is a multi-hospital delivery and health care system serving parts of Wisconsin, Iowa, and Illinois. UnityPoint was the victim of a "phishing attack" data breach that compromised Plaintiff's and other Class Members' protected health information from

as far back as November 1, 2017. UnityPoint reportedly discovered the data breach between February 7, 2018 and February 15, 2018.

2. On or about April 17, 2018 Plaintiff received a letter notifying her she was one of Defendant's patients affected by the breach. The letter informed Plaintiff that Defendant wanted to make Plaintiff aware of the situation so she could take precautionary measures to protect her health information.

3. In the letter, UnityPoint suggested steps that individuals can take to protect their medical information. The notification letter did not mention whether Defendant would offer protective services such as credit and identity theft protection.

4. Plaintiff Fox, and the patients and consumers she seeks to represent, are victims of UnityPoint's negligence and unfair practices who have suffered tangible injury-in-fact. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit and seeks injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in the possession of Defendant.

JURISDICTION AND VENUE

5. This Court has original jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because: (a) at least one member of the putative Class is a citizen of a state different from UnityPoint; (b) the amount in controversy exceeds \$5,000,000, exclusive of interest and costs; (c) the proposed Class consists of more than 100 Class Members; and (d) none of the exceptions under the subsection apply to this action.

6. Pursuant to 28 U.S.C. § 1367 (supplemental jurisdiction over pendant state law claims), this Court has supplemental jurisdiction over the Wisconsin health information, privacy,

and deceptive practices laws, including Wis. Stat. §§ 146.81, *et seq.*, Wis. Stat. §§100.18, *et seq.*, and other state statutory and common law claims.

7. This Court has personal jurisdiction over Defendant because: (a) it is registered to, and in fact does, conduct business in Wisconsin; and (b) has sufficient minimum contacts in Wisconsin, or otherwise intentionally avails themselves of the markets within Wisconsin through the promotion, sale, marketing, and distribution of its services, to render the exercise of jurisdiction by this Court proper and necessary.

8. Venue is proper in this District under 28 U.S.C. § 1391 because: (a) Plaintiff is a resident of, and domiciled in, this District; (b) Defendant conduct substantial business in this District; and (c) a substantial part of the events giving rise to Plaintiff's claims alleged herein occurred in this District.

PARTIES

9. Plaintiff Yvonne Mart Fox is a natural person and citizen of the state of Wisconsin, residing in Middleton, Wisconsin.

10. Defendant Iowa Health System, Inc. 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 Dane County, the state of Wisconsin, and the states of Iowa and Illinois. Defendant does business as UnityPoint Health. At all times material to this action, acting alone or in concert with others, Unity Point has advertised, marketed, distributed, and sold its health care services to patients and consumers in the state of Wisconsin and in the states of Iowa and Illinois.

COMMON FACTUAL ALLEGATIONS

11. Defendant UnityPoint (known as Iowa Health System until 2013) is a network of

hospitals, clinics, home care services, and health insurers in Wisconsin, Iowa, and Illinois. Defendant's health system now encompasses eight metropolitan areas in three states.

12. At least as early as the period between February 7, 2018 and February 15, 2017, UnityPoint discovered it had suffered one or more "phishing attacks" via one or more employee email account(s) (the "Privacy Breach" or "Privacy Breaches") that compromised access to 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, and other financial information (the "Personal Health Information" or "PHI"),

13. The Privacy Breach exposed PHI that was accessed and stolen from as far back as November 1, 2017. Defendant claims the Privacy Breach went undetected for several months. Upon discovery, rather than immediately disclose the Privacy Breaches and inform patients, the public, and regulators of what occurred, UnityPoint waited more than two months before it acknowledged PHI had been stolen.

14. UnityPoint ultimately disclosed the Privacy Breach to the consumers and the public on or about April 16, 2018. However, in an effort to minimize the harm, UnityPoint did not disclose all the true facts about the Privacy Breach.

15. In a notification form letter to affected patients dated April 16, 2018 (the "Notice Letter" or "Letter"), UnityPoint falsely claimed, "The information did not include your Social Privacy number." The Notice Letter went on to say, [w]e want to make impacted individuals aware of the situation so they can take precautionary measures to protect their health information."

16. The Notice Letter then further falsely claimed UnityPoint had no information

indicating that the stolen PHI "will be used for any unintended purposes." Defendant's Letter then listed some practices "[a]s a general matter" that individuals can take to protect their personal information and PHI.

17. Plaintiff, who has been a patient of UnityPoint and its affiliates since at least September 17, 2015, received a copy in the mail of the Notice Letter on or about April 17, 2018. The Notice Letter did not state how many persons had their PHI compromised, the size and complete scope of the Privacy Breach, whether Defendant would pay to or otherwise take precautionary measures to mitigate its patients' injury, or whether Defendant would offer protective services such as credit and identity theft protection.

18. The Privacy Breach is not the first evidence of UnityPoint's failure to secure patient PHI during the last 24 months. 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 HSS on May 25, 2017 of an email hacking/IT incident affecting 2,036 individuals.¹

19. Compromised PHI is a one of the most valuable commodities on the criminal information black market. In 2014, the FBI warned healthcare organizations that PHI data is worth 10 times the amount of personal credit card data on the black market.² PHI data for sale is so valuable because PHI information is so broad, and it can therefore be used for a wide variety of

¹ UnityPoint and UW Health received regulatory approval from the Federal Trade Commission approval for their joint operating agreement on or about April 11, 2017.

² Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained his data by monitoring underground exchanges where hackers sell the information.

criminal activity such as to create fake IDs, buy medical equipment and drugs that can be resold on the street, or combine patient numbers with false provider numbers to file fake claims with insurers.

20. The value of Plaintiff's and the Class Members' PHI on the black market is considerable. Stolen PHI 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.

21. It can take patients years to spot healthcare identity or PHI theft, giving criminals plenty of time to milk that information for as much cash as possible. That is precisely what makes medical data PHI more desirable to criminals than credit card theft. Credit card or financial information theft can be spotted by banks early on, and accounts can be quickly frozen or cancelled once the fraud is detected, making credit card and financial data much less valuable to criminals than PHI.

22. By way of the Privacy Breach, Defendant has deprived Plaintiff and Class Members of the substantial value of their PHI. Defendant has given access to the PHI of Plaintiff and the Class Members for criminals to use in the conduct of criminal activity. And, Defendant has opened up and exposed the email addresses and telephone numbers of Plaintiff and the Class Members to persons engaged in disruptive and unlawful business practices and tactics, including spam emails, robo-dialed calls, junk texts and faxes, and other unwanted calls and communications.

23. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up to date technology security strategy, demonstrates a willful and conscious disregard for patient and consumer privacy

and has exposed the private information and PHI of Plaintiff and at least 16,429 Class Member users of UnityPoint's services to unscrupulous operators, con artists, and outright criminals.

24. Rather than taking steps to fairly and fully inform Plaintiff and the Class Members about the true facts regarding the Privacy Breach and take "precautionary measures" to mitigate the cost and injury to affected patients, Defendant instead misrepresented the nature, breadth, scope, harm, and cost of the Privacy Breach to Plaintiff and the Class Members when it falsely stated in the Notice letter that, "The [stolen] information did not include your Social Privacy number", and "We 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."

25. Defendant knew, or should have known, that the stolen information did include affected patient Social Security numbers.³ Defendant further knew, or should have known, it possessed information that makes it highly likely the PHI 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 Privacy Breach.

PLAINTIFF FOX'S EXPERIENCE

26. Plaintiff Yvonne Mart Fox is a resident of Middleton, Wisconsin. Ms. Fox has been a patient and user of UnityPoint and its affiliates' services since at least September 17, 2015. During the time Ms. Fox was a UnityPoint patient, she did not use the UnityPoint internet portal to see her PHI or to contact her physicians or their offices. Similarly, she did not communicate

³ Insurance information, which UnityPoint admits was stolen, includes Medicare claim numbers which are the Social Security number of the primary wage earner on which benefits are based, plus an appropriate letter code.

over the internet with UnityPoint or her physicians or their offices. Everything was done by phone or U.S. postal service mail.

27. Commencing in and around the first quarter of 2018 Plaintiff began to notice an increase in the amount of unsolicited auto-dialed or "robo-dialed" phone calls, "spam" emails, and unsolicited marketing and promotional communications on her mobile and landline telephones. Plaintiff's mobile phone or data plan is limited, and unwanted junk texts or autodialed calls cause Plaintiff injury by restricting her available use.

28. On or about April 17, 2018, Plaintiff Fox received a copy of the Notice Letter containing the misrepresentations and omission set forth herein in the mail signed by RaeAnn Isaacson, Privacy Officer, UnityPoint Health. Plaintiff then called UnityPoint on April 24, 2018 and spoke with a UnityPoint employee or representative named Ashley.

29. Plaintiff inquired about the size and nature of the PHI, what specific PHI had been compromised in the Breach, and what type of precautions UnityPoint was recommending. In response, Ms. Ashley resorted to a scripted reply apologizing for the Privacy Breach and repeating over and over the mantra that Plaintiff Fox "should take steps to protect her information."

30. Plaintiff told Ms. Ashley that she already did not use the internet to communicate with UnityPoint or review her records, and in response again received the same mantra from Ms. Ashley, namely "We are sorry, please take precautions to protect your information." Plaintiff then asked if UnityPoint would pay for any precautions they were advising be taken in connection with the Privacy Breach. Once again, Ms. Ashley repeated the exact same script: "We are sorry, please take precautions to protect your information."

31. Plaintiff then asked to speak to a supervisor, and Ms. Ashley said she would try to reach one. When Ms. Ashley came back on the line Plaintiff was told a supervisor would call her back in a few days.

32. Plaintiff told Ms. Ashley she did not want to wait "a few days" and was again met with the scripted words, "We are sorry, please take precautions to protect your information." Frustrated in her efforts to obtain information by UnityPoint's stonewalling, Plaintiff said goodbye to Ms. Ashley and hung up the phone

33. Within 15 minutes, Plaintiff received a call from the number (503) 350-5979. The call was from someone purporting to be "Sujea" [sic] calling on UnityPoint's behalf. Once again, in response to Plaintiff's questions as set forth above, Ms. Sujea repeated the mantra: "We are sorry, please take precautions to protect your information."

34. Ms. Sujea repeated the mantra several times, only this time when Plaintiff asked if UnityPoint would pay for any reasonably appropriate precautions to mitigate the injury and harm from the Privacy Breach, Plaintiff Fox was told there would be no further remedial action from UnityPoint and no assistance or monetary compensation.

35. As a result of the Privacy Breach, Plaintiff is being inundated with unwanted, unsolicited, and unlawful spam emails and auto-dialed calls from unscrupulous operators. These calls not only restrict Plaintiff's mobile phone usage, but also amounts of Plaintiff's phone battery and the costs of the electricity needed to recharge her mobile phone. These spam emails and robo-dialed calls also cause Plaintiff annoyance, frustration, and wasted time. Plaintiff's privacy is being invaded as a direct result of the Privacy Breach, and she and her property rights are being caused harm without her permission.

36. Because it can take years to spot healthcare identity or PHI theft, Plaintiff is forced to purchase identity theft insurance and keep it in force indefinitely to mitigate the injury and harm caused by the Privacy Breach. Aside from the most obvious financial loss consequence, both direct and indirect, that Plaintiff is encountering, identity theft negatively impacts credit scores.⁴ Because a criminal's delinquent payments, cash loans, or even foreclosures slowly manifest into weakened credit scores, and because this type of fraud takes the longest time to resolve, Plaintiff is forced to purchase credit monitoring services indefinitely.

37. Identity theft is not only impacting Plaintiff financially, but also is taking a significant emotional toll. Plaintiff, like other PHI theft victims, fears for her personal financial security and is experiencing daily feelings of rage and anger as well as sleep disruption. As Plaintiff puts it, "It feels like I'm having surgery in public."⁵

CLASS ACTION ALLEGATIONS

38. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3) on behalf of herself and all Members of the Class and Subclass defined as:

⁴ Direct financial loss refers to the amount of money stolen or misused by the identity theft offender. Indirect financial loss includes any outside costs associated with identity theft, like legal fees or overdraft charges. A 2014 Dept. of Justice study found that victims experienced a combined average loss of \$1,343. In total, identity theft victims lost a whopping \$15.4 billion in 2014.

⁵ A 2013 survey from the Identity Theft Research Center reports that from an emotional standpoint, the impact of identity theft for some victims continues to be traumatic, as evidenced by their answers. Participant responses covered a broad range of emotions, including suicidal feelings (6.7 percent), shame or embarrassment (29.4 percent), overwhelming sadness (31.6 percent) and disbelief (41.2 percent). Much higher percentages of helplessness (50.3 percent) betrayal (50.8 percent), and rage and anger (65 percent) may be indicative of complex issues involving other types of identity theft, not just financial. Nearly 70 percent of the respondents indicated fear regarding their own personal financial security.
http://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf (last view May 4, 2018)

The PHI Breach Class. All persons in the United States whose Personal Health Information was accessed by third parties in the November 2017 to February 2018 Privacy Breach.

The Notice Letter Class. All persons who were mailed and received the Notice Letter.

The Classes described in this Complaint may be jointly referred to as the “Class” and proposed Members of the Classes may be jointly referred to as “Class Members.”

39. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant’s subsidiaries, parents, successors, predecessors, affiliates, and any entity in which the Defendant or its parent has a controlling interest, and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff’s counsel and Defendant’s counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

40. Plaintiff and the Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 23 of the Federal Rules of Civil Procedure.

41. **Numerosity:** The exact number of members of the Class is unknown, but is estimated to be at least 16,429 at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendant’s records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other consumer breach of contract, unlawful trade practices, and class action controversies.

42. **Typicality:** Plaintiff's claims are typical of the claims of other members of the Class, in that Plaintiff and the Class Members sustained damages all arise out of Defendant's Privacy Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and the Class Members sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

43. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with or are antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff.

44. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

- a. whether Defendant violated the Wisconsin Confidentiality of Patient Health Care Records laws, Wis. Stat. §§ 146.81, *et seq.*;
- b. whether Defendant had a duty to use reasonable care to safeguard Plaintiff's and the Class Members' PHI;
- c. whether Defendant breached the duty to use reasonable care to safeguard Class Members' PHI;
- d. whether UnityPoint breached its contractual promises to safeguard Plaintiff's and the Class Members' PHI;
- e. whether Defendant was negligent *per se* in not complying with federal and state privacy laws;

- f. whether Defendant violated the Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§100.18, *et seq.*;
- g. whether Defendant had a duty to disclose the truth about the Privacy Breach in connection with affected patients' PHI;
- h. whether Defendant knew or should have known their practices and representations related to the Notice Letter, Privacy Breach, and PHI were deceptive and unfair;
- i. whether Defendant is liable for negligence or gross negligence;
- j. whether Defendant's conduct, practices, statements, and representations about the Privacy Breach of the PHI violated applicable state laws;
- k. whether Defendant knew or should have known their representations were false, deceptive, unfair, and misleading;
- l. whether Defendant concealed material information regarding the true breadth, scope, and nature of the PHI compromised and stolen in the Privacy Breach;
- m. whether Plaintiff and the Class Members were damaged as a proximate cause or result of the Privacy Breach
- n. whether Plaintiff and the Class Members were damaged as a proximate cause or result of and Defendant's breaches of its contract with Plaintiff and the Class Members;
- o. whether Defendant's practices and representations related to the Privacy Breach that compromised the PHI breached implied warranties;
- p. whether Defendant have been unjustly enriched as a result of the conduct complained of herein;
- q. what is the proper measure of damages; and
- r. whether Plaintiff and the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

45. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of

this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be fostered and uniformity of decisions ensured.

46. A class action is therefore superior to individual litigation because:

- a. the amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the Class action procedure;
- b. individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and
- c. the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

47. In addition to satisfying the prerequisites of FRCP 23(a), Plaintiff satisfies the requirements for maintaining a class action under FRCP 23(b)(2) and (3). Class certification is appropriate under FRCP Rule 23(b)(1) or (b)(2) because:

a. the prosecution of separate actions by the individual Members of the proposed Class would create a risk of inconsistent or varying adjudication which 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

c. Defendant has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Class as a whole.

COUNT I
Negligence
On Behalf of Plaintiff and the Classes

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

49. Plaintiff and Class Members entrusted their PHI to Defendant. Defendant owed to Plaintiff and the other Class Members a duty to exercise reasonable care in handling and using PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Privacy Breach, theft, and unauthorized use, and to promptly detect attempts at unauthorized access.

50. Defendant owed a duty of care to Plaintiff and Class Members because Plaintiff and Class Members were foreseeable and probable victims of using email, and negligent, insecure emailing practices, to transmit and send confidential PHI. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PHI by

providing access to this information to third parties and by failing to properly supervise the manner in which the PHI was stored, used, and exchanged.

51. Defendant owed to Plaintiff and the Class Members 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 Wis. Stat. § 134.98. Defendant also owed a duty to timely and accurately disclose to Plaintiff and the other Class Members the scope, nature, and occurrence of the Privacy Breach. This duty is required and necessary in order for Plaintiff and the other Class Members 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 Privacy Breach.

52. Defendant owed these duties to Plaintiff and the other Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact by Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the other Class Members' personal information and PHI. Plaintiff and the other Class members were required to provide their personal information and PHI to Defendant in order to obtain services, and Defendant retained the information throughout Plaintiff's and the other Class members' use of Defendant's services.

53. The risk that unauthorized persons would attempt to gain access to the PHI was foreseeable. As the holder of vast amounts of PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PHI.

54. Such information is highly valuable, and Defendant is aware of numerous instances when criminals have attempted to access, and in fact have accessed PHI from Defendant, its

affiliates, and others. Defendant has been targeted by criminals successfully in the past by such attempts. Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PHI of Plaintiff and the other Class Members, and the importance of exercising reasonable care in handling it.

55. Defendant breached its duties by failing to exercise reasonable care in handling and securing the personal information of Plaintiff and the other Class Members, which proximately caused the Privacy Breach and Plaintiff's and the other Class Members' injuries. Defendant further breached its duties by failing to provide timely and accurate notice of the Privacy Breach to Plaintiff and the other Class Members, which proximately caused and exacerbated the Privacy Breach, and Plaintiff's and the other Class Members' injuries-in-fact. As a direct result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including embarrassment, humiliation, frustration, and emotional distress.

56. Defendant's breach of common law duties to exercise reasonable care and its failures and negligence proximately caused the Plaintiff's and other Class Members' actual, tangible injury-in-fact and damages, including without limitation the theft of their PHI by criminals, improper disclosure of their PHI, lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Privacy Breach that resulted and was caused by Defendant's negligence, which injury-in-fact and damages they continue to face.

COUNT II
Negligence *Per Se*
On Behalf of Plaintiff and the Classes

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

58. Pursuant to HIPAA and Wisconsin law (Wis. Stat. §§ 146.81, *et seq.*), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and the Class Members' PHI. Pursuant to several state laws, including but not limited to Wisconsin, Defendant had a duty to Plaintiff and Class Members' residing in those states to not disclose and to safeguard Plaintiff's and Class Members' confidential PHI.

59. Defendant breached its duties under state law to Plaintiff and the Class Members by providing access, exposing, and disclosing their information to third parties, and by failing to safeguard and provide adequate security for their PHI in an unreasonable manner. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

60. But for Defendant' negligence *per se*, breach of their duties ,and/or negligent supervision of their agents, contractors, vendors, and suppliers, Plaintiff and the Class Members would not have suffered injury-in-fact. The injury and harm suffered by Plaintiff and the Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that they were failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their confidential PHI.

61. As a direct and proximate result of Defendant' negligent conduct and/or negligent supervision, Plaintiff and Class Members have been injured and are entitled to damages.

COUNT III

Breach of Confidentiality of Health Records, Wis. Stat. 146.81, *et seq.* On Behalf of Plaintiff and the Classes

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

63. Wisconsin law regarding Confidentiality of Patient Health Care Records, Wis. Stat. §§ 146.81, *et seq.*, states that:

“All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient.” Wis. Stat. § 146.82.

64. The stolen PHI belonging to Plaintiff's and the Class Members are "Health care records" under Wis. Stat. § 146.81(4).⁶

65. Defendant violated Wis. Stat. §§ 146.81, *et seq.* when it compromised, allowed access to, and released, patient health care records and PHI to third parties without the informed consent or authorization of Plaintiff and the Class Members. Defendant did not and does not have express or implied consent to allow access to, or release of, Plaintiff's and the Class Members' PHI. To the contrary, Defendant expressly undertook a duty and obligation to Plaintiff and Class Members when it told them their PHI would be private and secure.

66. Defendant did not disclose to or warn Plaintiff and Class Members that their PHI could be compromised, released, or disclosed to third parties without their consent as a result of Defendant's computer systems and software being outdated, easy to hack, inadequate, and insecure. Plaintiff and Class Members did not know or expect, or have any reason to know or suspect, that Defendant's computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their PHI to unauthorized disclosure. In fact, they were told to the contrary in written statements and representations given to Plaintiff and Class Members, and on Defendant's website, namely that,

⁶ "'Patient health care records' means all records related to the health of a patient prepared by or under the supervision of a health care provider; . . ." Wis. Stat. § 146.81(4).

"[UnityPoint] 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." [*Emphasis added.*]

And,

"*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." [*Emphasis added.*]

And,

"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."

67. Wis. Stat. § 146.84(1)(b) states,

Any person, including the state or any political subdivision of the state, who violates Wis. Stat. s. 146.82 or 146.83 in a manner that is knowing and willful shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than \$25,000 and costs and reasonable actual attorney fees."

68. Wis. Stat. § 146.84(1)(bm) states,

"Any person, including the state or any political subdivision of the state, who negligently violates Wis. Stat. s. 146.82 or 146.83 shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than \$1,000 and costs and reasonable actual attorney fees." Wis. Stat. § 146.84(1)(bm).

69. Wis. Stat. § 146.84(1)(c) states,

"An individual may bring an action to enjoin any violation of s. 146.82 or 146.83 or to compel compliance with s. 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection."

70. Plaintiff and the Class request that the Court issue declaratory relief declaring Defendant's practice of using insecure, outdated, and inadequate email and computer systems and

software that are easy to hack for storage and communication of PHI data between Defendant and third parties unlawful. Plaintiff further requests the Court enter an injunction requiring Defendant to cease the unlawful practices described herein, and enjoining Defendant from disclosing or using PHI without first adequately securing or encrypting it.

71. Plaintiff and the Class Members request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing PHI of Plaintiff and the Class Members in their possession or the possession of third parties and provide it to Plaintiff and the Class Members.

72. Plaintiff and the Class Members request that the Court enter an injunction ordering that Defendant:

(a) engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct test, and audit Defendant's safeguards and procedures on a periodic basis;

(b) audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

(c) conduct regular checks and tests on its safeguards and procedures;

(d) periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response; and

(e) meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps *Defendant* is taking to update its security technology to adequately secure and safeguard patient PHI.

73. Plaintiff and the Class Members request the Court enter an order pursuant to Wis. Stat. § 146.84(1)(bm) awarding minimum statutory exemplary damages of \$1,000 to each

Plaintiff and each Class Member whose PHI was compromised, as well as attorneys' fees and costs.

COUNT IV
Invasion of Privacy
On Behalf of Plaintiff and the Classes

74. Defendant published private facts about Plaintiff and Class Members by disclosing and exposing Plaintiff's and Class Members' PHI through their negligent PHI security and retention practices.

75. The disclosure of the PHI, including treatment information, surgical information, diagnoses, lab results, the treatment received, and the medications taken would be offensive to a reasonable person of ordinary sensibilities.

76. The Plaintiffs' and Class Members' PHI is not a matter of legitimate public concern. As a direct and proximate result of Defendant' conduct, Plaintiff and Class Members have been injured and are entitled to damages.

COUNT V
Misrepresentation and Concealment
On Behalf of Plaintiff and the Notice Letter Class

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

78. Defendant knowingly made false and deceptive representations regarding its data security practices and policies, in its privacy statements and elsewhere, including enumerating specific uses and ways in which the PHI could be shared. Defendant additionally knowingly made false and deceptive statements in its Notice Letter and in statements and representations made to the public through press releases and on Defendant's website to cover up and conceal the breadth, scope, and nature of the Privacy Breach through knowing misrepresentations and omissions of

material fact.

79. On or about April 16, 2017, Defendant knowingly misrepresented the nature, breadth, scope, harm, and cost of the Privacy Breach to Plaintiff and the Class Members when RaeAnn Isaacson, Privacy Officer falsely stated on behalf of UnityPoint in the Notice Letter that "The [stolen] information did not include your Social Privacy number", and "We 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."

80. Defendant knowingly misrepresented in statements it made to the public on April 16, 2018 in press releases and on Defendant's website that the stolen PHI did not include affected patients' Social Security number. Defendant also knowingly made false and deceptive statements on April 16, 2018 to the public in press releases and on Defendant's website when it claimed UnityPoint had no information indicating that the stolen PHI will be used for any unintended purposes.

81. On April 16, 2018, in the Notice Letter, in press releases, and on Defendant's website, Defendant omitted the material fact that patients' Medicare numbers, and therefore Social Security numbers, are included in the compromised PHI. Defendant further knew, or should have known, it possessed information that makes it highly likely the PHI will be used for an unintended purpose. Defendant knowingly, intentionally, and recklessly made these false statements in an effort to minimize and conceal the harm and injury-in-fact to Plaintiff and the Class Members caused by the Privacy Breach.

82. These knowing misrepresentations and omissions were intended to: (a) conceal, minimize, and obfuscate the true breadth, scope, and nature of the Privacy Breach; (b) delay the notification of an investigation into the amount of liability and cost Defendant is legally

responsible for to Plaintiff and the Class Members; and (c) induce the Plaintiff, Class Members, and the public to continue to use Defendant's services and/or increase consumption of Defendant's services.

83. Defendant's misrepresentations and omissions about the stolen Social Security numbers and likely use of the stolen PHI were untrue. Defendant made the representations knowing they were untrue or recklessly, without caring whether they were true or false. Defendant made these misrepresentations with intent to defraud and to induce Plaintiff and the Class Members to rely and act upon them. Plaintiff believed the statements to be true and relied on them to her detriment.

84. As a result of Defendant's false and misleading statements, Plaintiff and the other Class Members have suffered additional pecuniary loss and injury-in-fact, including without limitation lost benefit of their bargain, lost value of their PHI, and consequential injury from the lost time and money incurred to mitigate and remediate the effects of the Privacy Breach, which injury-in-fact and damages they continue to face.

COUNT VI
Breach of Contract
On Behalf of Plaintiff and the Classes

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

86. Defendant entered into binding and enforceable contracts with Plaintiff and the other Class Members, supported by consideration including the payment for services by Plaintiff and the Class Members. These contracts include terms covering privacy and limiting the use and sharing of Plaintiff's and the other Class Members' PHI. Plaintiff and the other Class Members

bargained for an adequate level of security and reasonable care with respect to the use, storage, and sharing of their PHI.

87. These contracts incorporated UnityPoint's privacy policies wherein UnityPoint promised to protect the privacy of Plaintiff's and Class Members' personal information in accordance with federal and state privacy laws, as well as their own privacy policies. Specifically, in a written document provided to Plaintiff and Class Members in connection with their health care services, and on Defendant's website, Defendant stated,

"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."

88. It was a violation of federal, state, and UnityPoint's privacy policies to disclose Plaintiff's and Class Members' highly confidential PHI 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 the bargain and instead received health care services that were less valuable than described in their contracts.

89. Plaintiff and the other Class Members performed their duties under the agreements. Defendant violated the terms of the contract by sharing Plaintiff's and the other Class Members' PHI for unauthorized purposes, without first obtaining Plaintiff's or the other Class Members' consent or encrypting the information in a form which could not reasonably be used to identify them.

90. 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 PHI, and notification to affected persons, including without limitation, HIPAA, the Wisconsin Health Information Privacy laws, and the Wisconsin Security Breach Notification laws. Plaintiff and Class Members have been injured as a result of Defendants' breach of contract and are entitled to damages.

91. 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 PHI, lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Privacy Breach, which injury-in-fact and damages they continue to face.

COUNT VII
Breach of Implied Covenant of Good Faith and Fair Dealing
On Behalf of Plaintiff and the Classes

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

93. The law implies a covenant of good faith and fair dealing in every contract. Defendant entered into a contract with Plaintiff and the other Class Members, which includes terms covering privacy and limiting the use and sharing of Plaintiff's and the other Class Members' PHI.

94. Plaintiff and the other Class Members performed their duties under the agreements. Defendant's unlawful and bad faith conduct, as described above, constitutes a breach of the implied covenant of good faith and fair dealing.

95. As a result of Defendant's unlawful misconduct and its breach of the covenant of good faith and fair dealing owed to Plaintiff and the Class Members, Plaintiff and the Class Members have suffered additional pecuniary loss and injury-in-fact, including without limitation lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Privacy Breach, which injury-in-fact and damages they continue to face.

COUNT VIII

Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§100.18, *et seq.* On Behalf of Plaintiff and the Notice Letter Class

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

97. Defendant's conduct violates Wisconsin's Deceptive Trade Practices Act, Wis. Stat. §100.18 ("WDTPA"), which provides that no,

"firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

Plaintiff and the Class Members "suffer[ed] pecuniary loss because of a violation" of the WDTPA. Wis. Stat. § 100.18(11)(b)(2).

98. Defendant deliberately engaged in deceptive and unlawful practices on April 16, 2018 when it issued announcements, statements, and representations, including in press

releases, on Defendant's website, and in the Notice Letter, in violation of Wisconsin law by representing to Plaintiff and the Class Members and the public that the PHI information compromised in the Privacy Breach did not include affected patients' Social Privacy number, when in fact Defendant knew that it does.

99. Defendant deliberately engaged in deceptive and unlawful practices on April 16, 2018 when it issued announcements, statements, and representations, including in press releases, on Defendant's website, and in the Notice Letter, in violation of Wisconsin law by representing to Plaintiff, the Class Members, and the public that Defendant had no information indicating that the stolen PHI will be used for any unintended purposes, when in fact, they did have such information and knowledge.

100. Plaintiff and the Class Members relied upon Defendant's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

COUNT IX
Unjust Enrichment
On Behalf of Plaintiff and the Classes

101. Plaintiff pleads this count in the alternative and incorporates the above allegations as if fully set forth herein.

102. Plaintiff and the other Class Members conferred a monetary benefit on Defendant in the form of money paid for the purchase of services from Defendant. Defendant appreciates or has knowledge of the benefits conferred directly upon them by Plaintiff and the other members of the Class.

103. Defendant knew about the Privacy Breach, its own deficiencies in security practices

that caused it, and its own course of conduct in covering it up through false and misleading statements and omissions.

104. It would be inequitable for Defendant to retain these benefits and there is no adequate remedy at law. Plaintiff and the other Class Members are therefore entitled to restitution, disgorgement, and imposition of a constructive trust.

COUNT X
Declaratory Relief
On Behalf of Plaintiff and the Classes

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

106. Defendant acted or refused to act on grounds that apply generally to Plaintiff and the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole within the meaning of Fed. R. Civ. P. 23.

107. Plaintiff seeks a declaration that Defendant's acts and omissions as alleged herein violates applicable State law, including without limitation the WDTPA, as well as such other and further relief as may follow from the entry of such a judgment.

PRAYER FOR RELIEF

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

A. Certify this case as a Class action on behalf of the Class defined above, appoint Yvonne Mart Fox as Class representative, and appoint the Law Office of Robert L. Teel as Class counsel;

B. Declare that Defendant is financially responsible for notifying all Class Members of the false and untrue nature of the Notice Letter in connection with the Privacy Breach and stolen PHI and provide them full, fair, adequate, and truthful notice thereof;

C. Award declaratory and other equitable relief, including rescission, as is necessary to protect the interests of Plaintiff and the Class Members;

D. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class Members;

E. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Privacy Breach and the stolen PHI;

F. Enter an award in favor of Plaintiff and the Class Members that includes compensatory, exemplary, punitive damages, and statutory damages, including pre and post interest thereon, in an amount to be proven at trial;

G. Award restitution and damages to Plaintiff and the Class Members in an amount to be determined at trial;

H. Order disgorgement of Defendant' unjustly acquired revenue, profits, and other benefits resulting from their unlawful conduct for the benefit of Plaintiff and the Class Members in an equitable and efficient manner determined by the Court;

I. Order the imposition of a constructive trust upon Defendant such that its enrichment, benefit, and ill-gotten gains may be allocated and distributed equitably by the Court to and for the benefit of Plaintiff and the Class Members.

J. Enter an award of attorneys' fees and costs, as allowed by law;

K. Enter an award of pre-judgment and post-judgment interest, as provided by law;

L. Grant Plaintiff and the Class leave to amend the Complaint to conform to the evidence produced at trial; and

M. Grant such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

Dated: May 4, 2018

/s/ Robert L. Teel

Robert L. Teel (Bar ID 127081)

LAW OFFICE OF ROBERT L. TEEL

lawoffice@rlteel.com

1425 Broadway, Mail Code: 20-6690

Seattle, Washington 98122

Telephone: 866.833.5529

Facsimile: 855.609.6911

Attorney for Plaintiff and the Proposed Class

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

YVONNE MART FOX

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

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

Robert Teel, Law Office of Robert L. Teel
1425 Broadway, Mail Code: 20-6690
Seattle, WA 98122

DEFENDANTS

IOWA HEALTH SYSTEM, INC., doing business as UNITYPOINT
HEALTH, an Iowa non-profit corporation
County of Residence of First Listed Defendant Dallas County, Iowa

(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys (If Known)

Unknown

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

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

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

- | | PTF | DEF | | PTF | DEF |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State | <input checked="" type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input checked="" type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input checked="" type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

28 U.S.C. § 1332(d) - Class Action Fairness Act

Brief description of cause:

Class Action Fairness Act action for Breach of Confidentiality of Health Records and related claims

VII. REQUESTED IN COMPLAINT:

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

DEMAND \$

Exceeds \$5,000,000

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

May 4, 2018

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
 United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
 United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
 Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
 Original Proceedings. (1) Cases which originate in the United States district courts.
 Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
 Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
 Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
 Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
 Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

Signature of Clerk or Deputy Clerk

AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. **18-cv-327**

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____.

☐ I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____; or

☐ I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____, and mailed a copy to the individual's last known address; or

☐ I served the summons on *(name of individual)* _____, who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____; or

☐ I returned the summons unexecuted because _____; or

☐ Other *(specify)*:

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ 0.00.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc:

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [UnityPoint Health Security Breach Sparks Lawsuit in Wisconsin](#)
