IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

RICHARD FAIRCLOTH, individually and on behalf of a class of similarly situated individuals,

Plaintiff,

v.

ADVENTIST HEALTH SYSTEM/SUNBELT, INC., d/b/a FLORIDA HOSPITAL, also d/b/a FLORIDA HOSPITAL ALTAMONTE, also d/b/a FLORIDA HOSPITAL ORLANDO, also d/b/a FLORIDA HOSPITAL APOPKA, also d/b/a FLORIDA HOSPITAL EAST ORLANDO, also d/b/a FLORIDA HOSPITAL CELEBRATION HEALTH, also d/b/a FLORIDA HOSPITAL KISSIMMEE, also d/b/a WINTER PARK MEMORIAL HOSPITAL, also d/b/a FLORIDA HOSPITAL CARDIOVASCULAR INSTITUTE, also d/b/a FLORIDA HOSPITAL CENTRA CARE, also d/b/a FLORIDA HOSPITAL HEART & VASCULAR INSTITUTE, also d/b/a FLORIDA HOSPITAL HEARTLAND MEDICAL CENTER, also d/b/a FLORIDA HOSPITAL HEARTLAND MEDICAL CENTER LAKE PLACID, also d/b/a FLORIDA HOSPITAL MEDICAL CENTER, also d/b/a FLORIDA HOSPITAL REHABILITATION AND SPORTS MEDICINE: ALTAMONTE, also d/b/a FLORIDA HOSPITAL REHABILITATION AND SPORTS MEDICINE: EAST ORLANDO, also d/b/a FLORIDA HOSPITAL REHABILITATION AND SPORTS MEDICINE: LAKE MARY, also d/b/a FLORIDA HOSPITAL REHABILITATION AND SPORTS MEDICINE: OVIEDO, also d/b/a FLORIDA HOSPITAL REHABILITATION AND SPORTS MEDICINE: WINTER PARK, also d/b/a FLORIDA HOSPITAL REHABILITATION AND SPORTS MEDICINE: ORLANDO, also d/b/a FLORIDA

Case No. 6:13CV572-ORL-37TBS

CLASS ACTION COMPLAINT
INJUNCTIVE RELIEF SOUGH

JURY TRIAL DEMANDED

HOSPITAL SPORTS MEDICINE AND REHAB – METROWEST, also d/b/a FLORIDA HOSPITAL WAUCHULA, also d/b/a FLORIDA HOSPITAL/SOUTH,

Defendant.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL
INJUNCTIVE RELIEF SOUGHT

Plaintiff Richard Faircloth ("Plaintiff") brings this Class Action Complaint ("Complaint") against Adventist Health System/Sunbelt, Inc., d/b/a Florida Hospital, also d/b/a Florida Hospital Altamonte, also d/b/a Florida Hospital Orlando, also d/b/a Florida Hospital Apopka, also d/b/a Florida Hospital East Orlando, also d/b/a Florida Hospital Celebration Health, also d/b/a Florida Hospital Kissimmee, also d/b/a Winter Park Memorial Hospital, also d/b/a Florida Hospital Cardiovascular Institute, also d/b/a Florida Hospital Centra Care, also d/b/a Florida Hospital Heart & Vascular Institute, also d/b/a Florida Hospital Heartland Medical Center, also d/b/a Florida Hospital Heartland Medical Center Lake Placid, also d/b/a Florida Hospital Medical Center, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Altamonte, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: East Orlando, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Lake Mary, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Oviedo, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Winter Park, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Orlando, also d/b/a Florida Hospital Sports Medicine and Rehab – Metrowest, also d/b/a Florida Hospital Wauchula, also d/b/a Florida Hospital/South (hereafter "Florida Hospital" or "Defendant"), and alleges

as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Plaintiff Faircloth brings this class action lawsuit against Florida Hospital for failing to safeguard its patients' sensitive personal information, including their protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), social security numbers, and medical histories (collectively, "Sensitive Information").

2. Florida Hospital is a health care provider with 22 locations throughout the State of Florida.

3. As a health care provider, Florida Hospital is required to protect its patients' Sensitive Information by adopting and implementing the specific data security regulations and standards set forth under HIPAA.

4. In addition to its implied statutory obligation, Florida Hospital specifically promises to safeguard its patients' Sensitive Information in accordance with HIPAA regulations and standards through its privacy policy and patient agreements

5. However, Florida Hospital breached its statutory obligation and express promise by maintaining its patients' Sensitive Information in an electronic database that lacked crucial—and statutorily required—security measures and protocols, in addition to failing to adequately train or monitor its employees' access of patients' Sensitive Information.

6. Florida Hospital's failure to implement such safeguards resulted in the systematic and continuous breach of its patients' Sensitive Information. Beginning in 2009, certain outside individuals (lawyer referral services and chiropractors) paid emergency room intake employees at Florida Hospital's Celebration campus to search the entire Florida Hospital electronic database, access—without authorization—the Sensitive Information of Florida Hospital patients, and identify injured patients that had been involved in car accidents for their own solicitation purposes. Over the span of this two-year scheme, these intake employees at the Florida Hospital's Celebration campus were able to easily gain access to the Sensitive Information of over 740,000 Florida Hospital patients from all 22 campuses using nothing more than their employer-provided log-on credentials—even though they were not authorized to access such information, were presumably supervised in some capacity, and access to such information had nothing to do with their job responsibilities and duties.

7. While some security threats are unavoidable in a rapidly developing technological environment (and, indeed, underscore the need for modern and robust information security protections), Florida Hospital's failure to segment and control its database in accordance with long standing HIPAA security regulations and industry standard data protection protocols jeopardized its patients' Sensitive Information, and fell well short of the promises made through its patient agreements and privacy policies.

8. Accordingly, Plaintiff Faircloth alleges claims for breach of contract, breach of implied contract, breach of implied covenant of good faith and fair dealing, unjust enrichment, and breach of fiduciary duty.

PARTIES

9. Plaintiff Richard Faircloth is a natural person and resident of Florida. Faircloth is a former patient of the Apopka campus of Florida Hospital. He was last admitted on January 25, 2010.

10. Defendant Adventist Health System/Sunbelt, Inc., d/b/a Florida Hospital, also d/b/a Florida Hospital Altamonte, also d/b/a Florida Hospital Orlando, also d/b/a Florida Hospital Apopka, also d/b/a Florida Hospital East Orlando, also d/b/a Florida Hospital Celebration Health, also d/b/a Florida Hospital Kissimmee, also d/b/a Winter Park Memorial Hospital, also d/b/a Florida Hospital Cardiovascular Institute, also d/b/a Florida Hospital Centra Care, also d/b/a Florida Hospital Heart & Vascular Institute, also d/b/a Florida Hospital Heartland Medical Center, also d/b/a Florida Hospital Heartland Medical Center Lake Placid, also d/b/a Florida Hospital Medical Center, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Altamonte, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: East Orlando, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Lake Mary, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Oviedo, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Winter Park, also d/b/a Florida Hospital Rehabilitation and Sports Medicine: Orlando, also d/b/a Florida Hospital Sports Medicine and Rehab – Metrowest, also d/b/a Florida Hospital Wauchula, also d/b/a Florida Hospital/South, is a Florida corporation incorporated in and existing under the laws of the State of Florida, with its principal place of business located at 900 Hope Way, Altamonte Springs, Florida 32714. Florida Hospital and its affiliates do business throughout the State of Florida.

JURISDICTION AND VENUE

11. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 1367 because Plaintiff's state law claims turn on substantial questions of Federal Law, specifically whether Florida Hospital violated HIPAA and its associated regulations, and his claims are so related that they forms part of the same case or controversy under Article III of the United States Constitution.

12. Venue is proper pursuant to 28 U.S.C. § 1391(b)(1)-(2) because Florida Hospital is a corporation headquartered in this judicial district and a substantial part of the events giving rise to Plaintiff's claims occurred in this judicial district.

FACTUAL BACKGROUND

Florida Hospital's Privacy Policy and Agreements to Keep Sensitive Information Confidential

13. Florida Hospital represented to Plaintiff and the Class that it would protect their Sensitive Information.

14. Through its website, Florida Hospital states the following confidentiality and privacy policy:

> **Notice of Patient Privacy Practices – "NPPP"**
>
> Medical information covered by this Notice is information that identifies you or could be used to identify you that is collected from you or created or received by Florida Hospital and that relates to your past, present or future physical or mental health condition, including health care services provided to you and payment for such health care services.
>
> * * *
>
> We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We

> create a record of the care and services you receive at the hospital. We need this record to provide you with quality care and to comply with certain legal requirements.

(*See* "Notice of Patient Privacy Practices" a true and accurate copy of which is attached hereto as Exhibit A.)

15. On its website, Defendant also enumerates the rights and responsibilities required of Florida Hospital and its patients:

> **Patients' Rights and Responsibilities**
>
> ***As a patient you have a right to:***
>
> Protection of your need for privacy and to receive care in a safe setting. Confidentiality of your health information.
>
> * * *
>
> ***As a patient you are responsible for:***
>
> Providing to your healthcare provider, to the best of your knowledge, accurate and complete information about present complaints, past illnesses, prior hospitalizations, medications and other matters related to your health.
>
> * * *
>
> Assuring that the financial obligations of your healthcare are fulfilled as promptly as possible.

(*See* "Patients' Rights and Responsibilities," a true and accurate copy of which is attached hereto as Exhibit B.)

16. Additionally, in recognizing the confidential and sensitive nature of the information it collects from patients, Florida Hospital adopted, and advertises on its website, a confidentiality policy with respect to Sensitive Information:

> Confidentiality
>
> Florida Hospital believes your health information is personal and confidential. We are committed to keeping your health information private, and we are legally required to respect your confidentiality.
>
> HIPAA is the Health Insurance Portability and Accountability Act, a Federal law that requires health providers to take certain steps to protect the privacy and security of patient health information.

(*See* "Patient Privacy" a true and accurate copy of which is attached hereto as Exhibit C.)

17. These representations and requirements are collectively provided on Florida Hospital's webpage that lists patients' responsibilities and rights. Florida Hospital created these representations and requirements and publicly advertised them on its website as a means of increasing the value of its services and the number of patients it receives and treats, thus allowing it to charge patients higher costs for treatment. This agreement is the same for all Florida Hospital patients, including Plaintiff and the Class.

Florida Hospital Fails to Properly Protect its Patients' Sensitive Information

18. As introduced above, Florida Hospital digitally stores patients' Sensitive Information on a commercial database on its servers, and promises through its patient agreements and privacy policies to protect such information using the standards set forth under HIPAA.

19. On July 5, 2006, Dale Munroe ("Munroe") was hired by Florida Hospital to work as a Registration Representative in the Emergency Department of the Celebration campus. Munroe's job description was simple and straightforward—register patients that came to the Celebration campus for emergency care.

20. To perform his job, Munroe was not required to access the Sensitive Information of any Florida Hospital patients other than as needed for patient registration at the Celebration campus.

21. Likewise, Munroe was not required to access the Sensitive Information of Florida Hospital patients that received health care from other campuses, as such information was at no time needed for patient registration at the Celebration campus.

22. Even though accessing Florida Hospital's patients' Sensitive Information was outside the scope of Munroe's job duties (*i.e.*, to register patients at the Celebration campus), Florida Hospital provided Munroe with log-on credentials that gave him broad access to the Sensitive Information of Florida Hospital's entire patient database from all 22 campuses.

23. Beginning in 2009, Munroe was paid by outside lawyer referral services and chiropractors to exploit Florida Hospital's lax data security—*i.e.*, by using Munroe's Florida Hospital database log-on credentials to identify and then disclose such patients' Sensitive Information for solicitation purposes.

24. As part of this scheme, Munroe used his log-on credentials to access the Sensitive Information of over 763,000 patients from all of Florida Hospital's campus locations over a span of two years.

25. In July of 2011, Florida Hospital finally fired Munroe after discovering that he had improperly accessed the patient records of a physician who had been fatally shot in a Florida Hospital parking garage.

26. Despite terminating Munroe for improperly accessing information stored on its supposedly secured databases (*i.e.*, the same location where patient Sensitive Information

is stored), Florida Hospital continued to make identical promises to its customers regarding the protection of their Sensitive Information, and Florida Hospital officials undertook no efforts to ascertain if Munroe had improperly accessed other patients' Sensitive Information or otherwise investigate/review Munroe's history of accessing patients' records whilst employed at the Celebration campus.

27. Further, after her husband's termination, Katrina Munroe—Munroe's wife, who was also an employee of Florida Hospital—continued what Munroe had started, and improperly accessed, viewed, and sold the Sensitive Information of Florida Hospital patients to these same third parties through August of 2011.

Florida Hospital Failed to Monitor Its Database And Enforce Its Existing (Albeit Deficient) Policies

28. Munroe's excessive and illicit access of patient Sensitive Information went uncorrected by Florida Hospital for two consecutive years.

29. To demonstrate the staggering breadth of Munroe's practice of improperly accessing patient Sensitive Information, an average Florida Hospital employee performing the same job as Munroe (*i.e.*, patient intake at one campus) would have accessed about 12,000 records during the same two-year span.

30. Incredibly, and thanks to Florida Hospital's wholly inadequate policies concerning the handling and security of its patients' Sensitive Information (including the oversight of those employees with access to such information), Munroe accessed over *763,000* patient records in that same period.

31. During this time, Florida Hospital employees (including Munroe) were permitted to, and often did, share their own unique log-in credentials and passwords to access patients' Sensitive Information, a practice that Munroe's supervisor was aware of and in fact condoned.

32. Further, Florida Hospital's information systems allowed for the log-in credentials and password of a single employee (like those assigned to Munroe) to be used to access multiple computers at the same time from multiple locations.

33. Despite having the capability to oversee and review Munroe's (or his wife's) access to patients' Sensitive Information—and having every reason to do so, particularly after terminating Munroe for illicitly accessing such Sensitive Information—Florida Hospital took no steps to do so.

Florida Hospital's Violated HIPAA and Industry-Standard Data Protection Protocols

34. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Sensitive Information, like the data left unguarded by Florida Hospital. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

35. Florida Hospital's data breach resulted from a combination of insufficiencies—especially pertaining to Florida Hospital's data security relating to its patients' Sensitive Information—that indicate Defendant did not comply with safeguards

mandated by HIPAA regulations and industry standards. Among other such insufficiencies, Defendant either failed to implement, or inadequately implemented, information security policies or procedures that (1) protected (*e.g.*, via encryption) or otherwise controlled the storage of Sensitive Information on Defendant's computers; (2) restricted access to such Sensitive Information to employees with proper security clearance or, at the very least, any actual need to access such Information; and/or (3) related to the supervision of employees with access to patient Sensitive Information.

36. In addition, Florida Hospital's prolonged data breach could have been prevented if Florida Hospital had honored its obligations to its patients by implementing HIPAA mandated, industry standard policies and procedures for securely maintaining Sensitive Information and ensuring only limited and appropriate access to such information.

37. Contributing to the problem was Florida Hospital's failure to effectively supervise and train its employees that were in charge of viewing, accessing, or otherwise supervising the use of the Sensitive Information of its patients.

38. Florida Hospital's security failures also include, but are not limited to, the following:

a. Failing to maintain an adequate data security system to prevent unauthorized access to Sensitive Information;

b. Failing to mitigate the risks of a data breach and unauthorized access to Sensitive Information;

c. Failing to encrypt or otherwise protect Sensitive Information of Plaintiff and Class members;

d. Failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1);

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

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

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

h. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

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

j. Failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(4);

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502 *et seq.*;

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

m. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

39. Florida Hospital also failed to comply with industry standards relating to data security. In March of 2005, the National Institute of Standards and Technology ("NIST") published a report detailing standards for healthcare providers to comply with HIPAA's Security Rule. In the Report, NIST recommends specific techniques to safeguard electronically stored Sensitive Information. In one example, NIST specifically recommends that providers "Implement Policies and Procedures for Authorizing Access" which includes "implement[ing] policies and procedures that . . . document, review, and modify a user's right of access to a workstation, transaction, program, or process."[1]

[1] MATTHEW SCHOLL ET AL., NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T OF COMMERCE. NIST SPECIAL PUBLICATION 800-66 REVISION 1, AN INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

40. In its report, NIST also discussed the proper means for establishing "Workstation Security" which included "Document[ing] the different ways workstations are accessed by employees and nonemployees," as well as how to maintain proper "Access Control" by determining, *inter alia*, how users access and use information and how much information they should be permitted to access at any given time.

41. In light of the foregoing, Florida Hospital has failed to comply with industry standards. Even more striking is that one of the exact examples recommended by NIST (*i.e.*, monitoring and limiting access to Sensitive Information, a free and commonly used technique), would have prevented the unauthorized access of patient Sensitive Information at Florida Hospital.

42. Even though Florida Hospital's patients both expected and paid for the above-described security measures as a part of their hospital experience (*i.e.*, that HIPAA mandated and industry standards would be used to protect of their Sensitive Information), they were not implemented, which resulted in the unauthorized access of their Sensitive Information.

Plaintiff Faircloth's Personal Experiences

43. On January 25, 2010, Plaintiff Faircloth was admitted as a patient to Florida Hospital's Apopka campus for treatment of his knee.

44. In order to receive treatment, Plaintiff Faircloth provided Florida Hospital with his Sensitive Information and entered into an agreement with Florida Hospital to receive health care. Faircloth expected that Florida Hospital would protect his Sensitive Information

---

SECURITY RULE, at 23 (2008), http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

using HIPAA's security regulations and industry standards.

45. Plaintiff paid Florida Hospital approximately $4,000 for his medical care and, among other aspects of his treatment, the protection of his Sensitive Information.

46. Had Plaintiff known of Florida Hospital's substandard security procedures and methods of protecting and storing his Sensitive Information, he would have paid substantially less for Florida Hospital's services.

47. Because Florida Hospital did not sufficiently protect his Sensitive Information, Plaintiff did not receive the entirety of the services he paid for and, as a result, he paid more than he otherwise would have based upon Florida Hospital's patient agreement and privacy policy.

48. At some point after Plaintiff was released from Florida Hospital on January 28, 2010 and the date that Munroe was terminated from his employment on July 12, 2011, Munroe accessed Plaintiff's Sensitive Information pursuant to the solicitation scheme described above.

CLASS ACTION ALLEGATIONS

49. Plaintiff brings this action on behalf of himself and a Class defined as follows:

> All individuals in the United States that are current or former patients of Florida Hospital and whose Sensitive Information was accessed without authorization by Dale Munroe or Katrina Munroe using the log-on credentials supplied by Florida Hospital.

Excluded from the Class are (i) any judge presiding over this action and members of their families; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and their current or former

employees, officers and directors; (iii) persons who properly execute and file a timely request for exclusion from the Class; and (iv) the legal representatives, successors or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of Florida Hospital's patient records.

50. **Numerosity:** The exact number of members of the Class is unknown to Plaintiff at this time, but on information and belief, there are at least 763,000 members of the Class throughout the country, making joinder of each individual member impracticable. Ultimately, the members of the Class will be easily identified through Defendant's records by, coincidentally, using the same information accessed without authorization by Munroe.

51. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and the Class sustained damages as a result of Defendant's uniform wrongful conduct during transactions with Plaintiff and the Class.

52. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff.

53. **Superiority:** This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. 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 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, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

54. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply and affect members of the Class uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff or any other Class member.

55. **Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual members, and include, but are not limited to:

a. Whether Defendant took steps and measures to necessary safeguard Plaintiff's and the Class members' Sensitive Information;

b. Whether Defendant breached its duty to protect Plaintiff's and the Class members' Sensitive Information by allowing an employee to

access, view, and steal this information in the manner alleged herein;

c. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiff and the members of the Class on the other, and the terms of those contracts;

d. Whether Defendant should retain the monies paid by Class members to protect their Sensitive Information;

e. Whether storing Sensitive Information in the manner alleged herein and failing to monitor access to such Information adhered to industry standards or HIPAA protocols; and

f. Whether and to what extent Plaintiff and the Class have sustained damages.

Plaintiff reserves the right to revise the Class definition based on facts learned in discovery.

COUNT I
Breach Of Contract
(On Behalf of Plaintiff and the Class)

56. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

57. Plaintiff paid money to Florida Hospital in exchange for its promise to provide patient services.

58. In addition to providing medical care, a material part of Florida Hospital's promise to provide patient services involved protecting his Sensitive Information.

59. In its written services contract as well as its patients' rights and privacy notices, Florida Hospital expressly promised Plaintiff and members of the Class that Florida Hospital only discloses health information when required to do so by federal or state law.

Florida Hospital further promised that it would protect his Sensitive Information.

60. Florida Hospital promised to comply with all HIPAA standards and to make sure that Plaintiff and the Class members' Sensitive Information was protected. Florida Hospital further promised to provide notice to Plaintiff and members of the Class describing Florida Hospital's legal duties and privacy practices with respect to their Sensitive Information.

61. The contracts required Defendant not to disclose Plaintiff's and the Class members' Sensitive Information to unauthorized third parties, and to safeguard the information from being lost and/or accessed without authorization.

62. Defendant did not safeguard Plaintiff's and the Class members' protected Sensitive Information. Specifically, Florida Hospital did not comply with its promise to abide by HIPAA and did not comply with industry standards.

63. The failure to meet these promises and obligations constitutes an express breach of contract.

64. Because Defendant allowed unauthorized access to Plaintiff's and the Class members' Sensitive Information and failed to safeguard their Sensitive Information, Defendant breached its contracts with Plaintiff and members of the Class.

65. A meeting of the minds occurred, as Plaintiff and members of the Class agreed, *inter alia*, to "[provide] to your healthcare provider, to the best of your knowledge, accurate and complete information about present complaints, past illnesses, prior hospitalizations, medications and other matters related to your health" and to pay Florida Hospital in exchange for Florida Hospital's agreement to, among other things, protect their

Sensitive Information. (Ex. B.)

66. Florida Hospital breached the contract by not meeting even a minimum level of protection of Plaintiff's and the Class members' Sensitive Information, because it did not prevent against the unauthorized access of 736,000 members' Sensitive Information that it promised to protect.

67. This failure to meet its confidentiality and privacy obligations resulted in Plaintiff and the Class receiving services from Florida Hospital that were of a diminished value.

68. Stated otherwise, because Plaintiff and the Class paid for privacy protections that they did not receive—even though such protections were a material part of their contracts with Florida Hospital—Plaintiff and the Class did not receive the full benefit of their bargain.

69. As a result of Florida Hospital's breach, Plaintiff and the Class suffered actual damages including, but not limited to, the diminished value of their paid-for health care services.

COUNT II
Breach of Implied Contract
(in the alternative to Breach of Contract)
(On Behalf of Plaintiff and the Class)

70. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 57-70.

71. In order to benefit from Defendant's services, Plaintiff and the Class disclosed Sensitive Information to Florida Hospital, including their names, contact information

(addresses, phone and fax numbers and email addresses), Social Security Numbers, dates of birth, and extremely sensitive medical diagnosis information.

72. By providing that Sensitive Information, and upon Defendant's acceptance of such information, Plaintiff and the Class, on the one hand, and Defendant, on the other hand, entered into implied contracts whereby Defendant was obligated to take reasonable steps to secure and safeguard that information.

73. Under the implied contract, Defendant was further obligated to provide Plaintiff and the Class with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

74. Without such implied contracts, Plaintiff and the Class would not have provided their personal information to Defendant.

75. As a result of Florida Hospital's breach, Plaintiff and the Class suffered actual damages including, but not limited to, the diminished value of their paid-for health care services.

COUNT III
Restitution/Unjust Enrichment
(in the alternative to Counts I and II)
(On Behalf of Plaintiff and the Class)

76. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 56-75.

77. Plaintiff and members of the Class conferred a monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiff and the Class in the form of health services fees.

78. Defendant appreciates or has knowledge of such benefit.

79. The health service fees that Plaintiff and the Class paid to Defendant were supposed to be used by Defendant, in part, to pay for the administrative costs of data management and security.

80. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and members of the Class, because Defendant failed to implement data management and security measures that Plaintiff and the Class paid for and are otherwise mandated by HIPAA and industry standards.

81. Further, as a result of Florida Hospital's conduct, Plaintiff and the Class suffered actual damages including, but not limited to, the diminished value of their paid-for health care services.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

82. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

83. As guardians of Plaintiff's and the Class members' Sensitive Information, Defendant owed a fiduciary duty to Plaintiff and the Class to: (1) protect their Sensitive Information; (2) timely notify them of any unauthorized access of that data; and (3) maintain complete and accurate records of what and where its members' Sensitive Information is stored.

84. Defendant breached its fiduciary duty to Plaintiff and the Class by:

a. Failing to diligently investigate the data breach to determine the number of members affected;

b. Failing to hire a forensics consultant to investigate the number of members affected, prevent future breaches from occurring, or mitigate any harm after the data breach occurred starting sometime in 2009, or even after Munroe was fired in July of 2011;

c. Failing to timely notify and/or warn Plaintiff and the Class members of the data breach;

d. Failing to ensure the confidentiality and integrity of electronic protected health information it created, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

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

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

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

h. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

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

j. Failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(4);

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502;

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

m. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c); and

n. Otherwise failing to safeguard Plaintiff's and the Class members' Sensitive Information.

95. As a result of Florida Hospital's conduct, Plaintiff and the Class suffered actual damages including, but not limited to, the diminished value of their paid-for health care services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for the following relief:

A. Certify this case as a class action on behalf of the Class as defined above, and appoint Richard Faircloth as Class Representative and undersigned counsel as Class Counsel;

B. Find that Defendant is liable under all legal claims asserted herein for its failure to safeguard Plaintiff's and the Class members' Sensitive Information;

C. Award injunctive and other equitable relief as is necessary to protect the interests of the Class, including: (i) an order prohibiting Florida Hospital from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Florida Hospital to protect all data collected through the course of its business in accordance with HIPAA and industry standards;

E. Award damages, including restitution, in an amount to be determined by an accounting of the difference between the price Plaintiff and the Class paid for Defendant's duty/promise to secure its members' Sensitive Information, and the actual services—*i.e.*, health care services devoid of paid-for data protection—rendered by Defendant, and punitive damages to Plaintiff and the Class in an amount to be determined at trial;

F. Award Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

G. Award Plaintiff and the Class pre and post-judgment interest to the maximum extent allowable by law; and

H. Award such other and further legal or equitable relief as equity and justice may require.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: April 9 2013

Respectfully submitted,

By: /s/Edmund A. Normand
One of Plaintiff's Attorneys

EDMUND A. NORMAND
ednormand@whkpa.com
Florida Bar No. 865590
WOOTEN, KIMBROUGH, & NORMAND, P.A.
236 South Lucerne Circle
Orlando, Florida 32801
Tel.: (407) 843-7060
Fax: (407) 843-5836
Service Email: normandeservice@whkpa.com
and ednormand@whkpa.com

JAY EDELSON (Trial Counsel)
jedelson@edelson.com
RYAN D. ANDREWS
randrews@edelson.com
ARI J. SCHARG
ascharg@edelson.com
BENJAMIN S. THOMASSEN
bthomassen@edelson.com
DAVID J. DALE
ddale@edelson.com
EDELSON LLC
350 North LaSalle, Suite 1300
Chicago, Illinois 60654
Tel.: (312) 589-6370
Fax: (312) 589-6378

Attorneys for Plaintiff