

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF FLORIDA**

**CASE No.: 1:15-cv-20683**

KELLIE LYNN CASE, individually and on  
behalf of all others similarly situated,

*Plaintiff,*

v.

HOSPITAL CORPORATION OF AMERICA,  
a West Virginia corporation, and ENVISION  
HEALTHCARE CORPORATION, a  
Delaware corporation,

*Defendants.*

---

**CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Kellie Lynn Case brings this Class Action Complaint and Demand for Jury Trial against Defendants Hospital Corporation of America and Envision Healthcare Corporation d/b/a Valesco Ventures (collectively, “Defendants”) and allege as follows upon personal knowledge as to herself and her own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

**NATURE OF THE ACTION**

1. Plaintiff brings this class action lawsuit against Defendants for their failure to safeguard their patients’ sensitive personal information, including, *inter alia*, their names, dates of birth, and protected health information as defined by the Health Insurance Portability and Accountability Act (“HIPAA”) (collectively, “Sensitive Information”).

2. Defendant Hospital Corporation of America is a health care provider that manages over 162 hospitals and 113 surgery centers throughout the world, including several in

the State of Florida (such as the Aventura Hospital and Medical Center facilities, located in the State of Florida). Defendant Hospital Corporation of America, together with Defendant Envision Healthcare Corporation, jointly work together to provide health care-related services to patients at Aventura Hospital.

3. As a health care provider, Defendants are required to protect their patients' Sensitive Information by adopting and implementing the specific data security regulations and standards set forth under HIPAA and Fla. Stat. Ann. § 395.3025(4). Many of these same data protection practices are mandated by industry standard data protection protocols.

4. In addition to their implied statutory obligations, Defendants—through Aventura Hospital's privacy policies and patient agreements—specifically promised to protect patients' Sensitive Information by adopting and implementing the specific data security regulations and standards set forth under HIPAA and Fla. Stat. Ann. § 395.3025(4).

5. Unfortunately, it took a large-scale medical data breach to reveal—*for the third time*—that Defendants failed to provide their patients' with the level of data protection that they promised and paid for.

6. Indeed, in September 2014, Defendants informed their patients that a hospital employee had been accessing—without authorization—the Sensitive Information of Aventura Hospital patients for nearly *two years*. Specifically, between September 13, 2012 and June 9, 2014, an employee was able to easily gain access to the Sensitive Information of thousands of Aventura Hospital patients—even though the individual was not authorized to access such information, was presumably supervised in some capacity, and access to such information had nothing to do with his or her 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), Defendants' failure to, *inter alia*, segment and control their databases in accordance with long standing HIPAA security regulations, Fla. Stat. Ann. § 395.3025(4), and industry standard data protection protocols jeopardized their patients' Sensitive Information, and fell well short of the promises made through Aventura Hospital's patient agreements and privacy policies.

8. Unfortunately, as a result of Defendants' failure to implement and follow basic security procedures, Plaintiff's Sensitive Information is now in the hands of thieves.

### **PARTIES**

9. Plaintiff Kellie Lynn Case is a natural person and resident of the State of Florida.

10. Defendant Hospital Corporation of America, d/b/a Aventura Hospital and Medical Center, is a corporation existing under the laws of the State of West Virginia with its headquarters and principal place of business located at 1 Park Plaza, Nashville, Tennessee 37203. Defendant Hospital Corporation of America's Aventura Hospital and Medical Center is located at 20900 Biscayne Boulevard, Aventura, Florida 33180. Defendant Hospital Corporation of America conducts business throughout this District, the State of Florida, and the United States.

11. Defendant Envision Healthcare Corporation, d/b/a Valesco Ventures, is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located at 6200 South Syracuse Way, Suite 200, Greenwood Village, Colorado 80111. Defendant Envision Healthcare Corporation conducts business throughout this District, the State of Florida, and the United States.

### **JURISDICTION AND VENUE**

12. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §

1332(d)(2) because (a) at least one member of the putative Class is a citizen of a state different from Defendants, (b) the amount in controversy exceeds \$5,000,000 exclusive of interest and costs, and (c) none of the exceptions under that subsection apply to this action.

13. This Court has personal jurisdiction over Defendants because they conduct business in Florida, have hospitals and other facilities located in Florida, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from Florida.

14. Venue is proper pursuant to 28 U.S.C. § 1391(b) because Defendants reside in this District, and because the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from Florida. Venue is additionally proper because Defendants maintain hospitals and other administrative offices in this District.

#### **FACTUAL BACKGROUND**

##### ***Defendants' Privacy Statements and Agreements Promise to Keep Patients' Sensitive Information Confidential***

15. Through their Notice of Privacy Practices (which all patients receive upon admission to their hospitals and facilities, and is generally available on Defendants' websites), Defendants represented that they would protect their patients' Sensitive Information and keep it confidential. For instance, the Notice of Privacy Practices stated in relevant part:<sup>1</sup>

“Each time you visit a hospital, physician, or other healthcare provider, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, a plan for future care or treatment, and billing-related information. This notice applies to all of the records of your care generated by the facility, whether made by facility personnel, agents of the facility, or your personal doctor . . . .”

---

<sup>1</sup> See *Aventura Hospital and Medical Center's Notice of Privacy Practices*, <http://aventurahospital.com/about/privacy-notice.dot> (last visited Sept. 17, 2014).

\* \* \*

“We are required by law to maintain the privacy of [such] health information, provide you a description of our privacy practices, and to notify you following a breach of unsecured protected health information. We will abide by the terms of this notice . . . Other uses and disclosures of health information not covered by this notice or the laws that apply to us will be made only with your written authorization.”

16. Similarly in Aventura Hospital’s Patient Rights and Responsibilities and Patient Visitation Rights, it asserts the following:

Patients shall have their “medical records, including all computerized medical information, kept confidential . . . .”<sup>2</sup>

17. Defendants’ statements about their data security and management practices—both through their privacy policies and public representations—served to falsely inflate the advertised utility of their services, thus allowing Aventura Hospital to charge patients higher costs for treatment.

***The Data Breach Revealed For The Third Time That Defendants’ Failed to Protect their Patients’ Sensitive Information as Promised***

18. As previewed above, Defendants digitally store patients’ Sensitive Information on a commercial database on their servers, and promised—through Aventura Hospital’s patient agreements and privacy policies—to protect such information using the standards set forth by law, including under HIPAA, Fla. Stat. Ann. § 395.3025(4), and in accordance with industry standards.

19. In September 2014, Defendants announced that—for the *third time* in the past several years—Aventura Hospital’s patient data had been compromised. Specifically, Defendants informed patients that, beginning in September 2012, an employee began to

---

<sup>2</sup> See *Aventura Hospital and Medical Center’s Patient Rights and Responsibilities and Patient Visitation Rights*, <http://aventurahospital.com/patients/patient-rights-and-responsibilities->

continuously and systematically use their databases to access and remove tens of thousands of their patients' Sensitive Information.

20. The excessive and unauthorized access of patients' Sensitive Information by the Aventura Hospital employee went uncorrected for *two consecutive years*.

21. Incredibly, and thanks to Defendants' wholly inadequate policies concerning the handling and security of their patients' Sensitive Information (including the oversight of those employees with access to such information), an employee—without authorization—was able to access over 85,000 patient records during that period.

***Defendants Violated HIPAA, Florida Law, and Industry Standard Data Protection Protocols***

22. HIPAA was enacted and became effective in 1996.

23. 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 Defendants. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

24. Additionally, Section 395.3025 of the Florida Statutes states that “Patient records are confidential and must not be disclosed without the consent of the patient or his or her legal representative,” save for limited exceptions not applicable here. Fla. Stat. Ann. § 395.3025(4).

25. Defendants' data breach resulted from a combination of insufficiencies—especially pertaining to Defendants' data security relating to their patients' Sensitive Information—that indicate Defendants did not comply with safeguards mandated by HIPAA

regulations, Florida law, or industry standards. That is, Defendants either failed to implement sufficient information security policies and procedures to (1) protect (*e.g.*, via encryption) or otherwise safeguard their patients' electronically-stored Sensitive Information; (2) restrict access (*i.e.*, segment) their electronic database to limit access to such Sensitive Information to only those employees and personnel that need to access such information for treatment related reasons; and (3) supervise employees and personnel with access to patient Sensitive Information and enforce their data protection and confidentiality policies.

26. In addition, Defendants' prolonged data breach could have been prevented if Defendants had honored their obligations to their patients by implementing even basic industry standard policies and procedures for securely maintaining Sensitive Information and ensuring only limited and appropriate access to such information.

27. Contributing to the problem was Defendants' failure to effectively supervise and train their employees that were in charge of viewing, accessing, or otherwise supervising the use of the Sensitive Information of their patients.

28. Defendants' 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 they 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 their 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 their workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their 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. Failing to ensure that their patients' medical records remain confidential and are not disclosed without consent of the patient or his or her legal representative, in violation of Fla. Stat. Ann. § 395.3025(4).

29. Defendants also failed to comply with industry standards relating to data security. For example, the National Institute of Standards and Technology ("NIST") published a report detailing standards for healthcare providers to come into compliance 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."<sup>3</sup>

---

<sup>3</sup> 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 Security Rule*, at 23 (2008), <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>.

30. In another example, NIST also discussed 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.<sup>4</sup>

31. The foregoing examples illustrate Defendants’ failure to comply with even basic 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, at-issue access of patient Sensitive Information at Defendants’ facilities.

32. Even though Defendants’ patients both expected and paid for the above-described security measures as a part of their health care-related experience (*i.e.*, that the practices mandated by HIPAA, Florida law, and industry standards would be used to protect their Sensitive Information), they were not implemented, which resulted in the unauthorized access of their Sensitive Information.

***Plaintiff Kellie Lynn Case’s Experience***

33. Prior to September 2014, Plaintiff Case was a patient at Defendants’ Aventura Hospital and Medical Center facilities in Florida.

34. As part of the patient-admission process, Case was required to provide Defendants with her Sensitive Information and agreed to receive and pay for services related to her health care. In return, Defendants promised to provide health care services and protect Case’s Sensitive Information in accordance with HIPAA, Fla. Stat. Ann. § 395.3025(4), and industry

---

<sup>4</sup> *Id.* at 38, 40.

standards.

35. Case paid Defendants for the health care services she received, which included, among other aspects of her treatment, the protection of her Sensitive Information.

36. Had Case known of Defendants' substandard security procedures and methods of protecting and storing her Sensitive Information, she would have paid substantially less for Defendants' health care services (*i.e.*, because the value of health care services *without* the adequate protection of Sensitive Information is worth substantially less than the value of such services *with* adequate protection) or would not have paid at all (*i.e.*, she would have sought care elsewhere).

37. Plaintiff's Sensitive Information was accessed by Defendants' employee as discussed *supra*, ¶¶ 19-21.

38. Because Defendants did not sufficiently protect her Sensitive Information, Case did not receive the entirety of the services she paid for and, as a result, she paid more than she otherwise would have.

### CLASS ALLEGATIONS

39. **Class Definition:** Plaintiff Case brings this action pursuant to Fed. R. Civ. P. 23(a), (b)(2) and (3) on behalf of herself and a class of similarly situated individuals, defined as follows:

All persons in the United States and its territories who (i) paid money to Defendants in exchange for health care services at Defendants' Aventura Hospital and Medical Center facilities and (ii) whose Sensitive Information was accessed as a result of the data breach that occurred between September 13, 2012 and June 9, 2014.

Excluded from the Class is (i) any judge presiding over this action and members of their families; (ii) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any

entity in which Defendants or their 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 Defendants' patient records.

40. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time, but on information and belief, there are tens of thousands of Class members throughout the country, making joinder of each individual member impracticable. Ultimately, the members of the Class will be easily identified through Defendants' records.

41. **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 Defendants adequately safeguarded Plaintiff's and the Class members' Sensitive Information;
- b. Whether Defendants' storage, maintenance, and protection of the Class members' Sensitive Information violated HIPAA's security protocols, Fla. Stat. Ann. § 395.3025(4), and/or industry standards;
- c. Whether implied or express contracts existed between Defendants, on the one hand, and Plaintiff and the members of the Class on the other;
- d. Whether Defendants' conduct described herein constitutes a breach of their contracts with Plaintiff and the Class members; and
- e. Whether Defendants should be permitted to retain the monies paid by Plaintiff and other Class members to protect their Sensitive Information.

42. **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 Defendants' uniform wrongful conduct during transactions with Plaintiff and the Class.

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 litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiff.

44. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because Defendants have 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. Defendants' policies challenged herein apply and affect members of the Class uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff or any other Class member.

45. **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 Defendants' wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' 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.

**FIRST CAUSE OF ACTION**  
**Breach of Express Contract**  
**(On Behalf of Plaintiff and the Class)**

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

47. Plaintiff and the Class members entered into valid and enforceable contracts (*i.e.*, patient contracts and incorporated or related agreements) with Defendants whereby Defendants promised to provide health care services to Plaintiff and the Class, and Plaintiff and the Class agreed to pay money for such services.

48. A material part of Defendants' promise to provide health care services to Plaintiff and the Class members was to protect their Sensitive Information.

49. In their written patient contracts, privacy policies, and other public representations, Defendants promised Plaintiff and the Class that they would comply with all laws relating to the maintenance of the privacy of patients' Sensitive Information, protect Plaintiff's and the Class members' Sensitive Information, and only disclose their health information when required by law.

50. Further, because the laws of the State of Florida are incorporated into every Florida contract—both as a matter of course and through the express representations made by Defendants—the contracts between Defendants and Plaintiff and the Class members included the obligation for Defendants to abide by Fla. Stat. Ann. § 395.3025(4), and as such, Defendants

were contractually obligated to keep patients' Sensitive Information confidential—even from their own employees and personnel, unless disclosure of such information is made in connection with their medical treatment or is otherwise expressly authorized by patients.

51. In sum, the contracts required Defendants to safeguard Plaintiff's and the Class members' Sensitive Information and to prevent disclosure and unauthorized access to such information.

52. Plaintiff and the Class members fulfilled their contractual obligations by paying Defendants for all aspects of their medical care and providing Defendants with accurate medical and financial information.

53. Defendants did not adequately safeguard Plaintiff's and the Class members' protected Sensitive Information. Specifically, Defendants failed to follow through on their promises to protect their patients' Sensitive Information in accordance with HIPAA, Fla. Stat. Ann. § 395.3025(4), and/or industry standards.

54. The failure to meet these promises and obligations constitutes an express breach of contract. In other words, Defendants breached the contracts with Plaintiff and the members of the Class by failing to implement sufficient security measures to protect Plaintiff's and the Class members' Sensitive Information as described herein.

55. This failure resulted in Plaintiff and the Class members receiving services that were of less value than they paid for (*i.e.*, the provision of medical care without adequate data security and protection).

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

bargain.

57. As a result of Defendants' breach, Plaintiff and the Class members suffered actual damages in the amount of the difference between the price they paid for Defendants' services as promised and the actual diminished value of their health care services.

**SECOND CAUSE OF ACTION**  
**Breach of Implied Contract**  
**(in the alternative to Breach of Express Contract)**  
**(On Behalf of Plaintiff and the Class)**

58. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 46–57.

59. In order to benefit from Defendants' services, Plaintiff and the Class paid money and disclosed Sensitive Information to Defendants, including their names, addresses, telephone numbers, Social Security numbers, dates of birth, and extremely sensitive medical diagnosis information.

60. By providing those payments and their Sensitive Information, and upon Defendants' acceptance of such payments and information, Plaintiff and the Class, on the one hand, and Defendants, on the other hand, entered into implied contracts whereby Defendants were obligated to take reasonable steps to secure and safeguard that information.

61. Under the implied contracts, Defendants were 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.

62. Without such implied contracts, Plaintiff and the Class would not have provided their Sensitive Information to Defendants.

63. As described herein, Defendants did not take reasonable steps to safeguard



Plaintiff's and the Class members' Sensitive Information.

64. Because Defendants allowed unauthorized access to Plaintiff's and the Class members' Sensitive Information and failed to take reasonable steps to safeguard their Sensitive Information, Defendants breached their implied contracts with Plaintiff and the Class.

65. The failure to meet these promises and obligations constitutes a breach of contract. In other words, Defendants breached the contracts by failing to implement sufficient security measures to protect Plaintiff's and the Class members' Sensitive Information as described herein.

66. Defendants' failure to fulfill their data security and management promises resulted in Plaintiff and the Class receiving services that were of less value than they paid for (*i.e.*, the provision of medical care without adequate data security and management practices).

67. 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 Defendants—Plaintiff and the Class did not receive the full benefit of their bargain.

68. As a result of Defendants' breach, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for Defendants' services as promised and the actual diminished value of their health care services.

**THIRD CAUSE OF ACTION**  
**Restitution/Unjust Enrichment**  
**(in the alternative to Counts I and II)**  
**(On Behalf of Plaintiff and the Class)**

69. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 46-68.

70. Plaintiff and the Class members conferred a direct monetary benefit on

Defendants. Defendants received and retained money belonging to Plaintiff and the Class in the form of health services fees.

71. Defendants received, retained, and benefited from Plaintiff's and other Class members' services fees to the detriment of Plaintiff and the Class.

72. Defendants appreciate or have knowledge of such receipt, retention, and benefit.

73. The health service fees that Plaintiff and the Class paid to Defendants are (or were to be) used by Defendants, in part, to pay for the administrative costs of data management, protection, and security.

74. Defendants knew or should have known that their data management and security measures were flawed and vulnerable, but did not utilize their patients' service fees to pay for the administrative costs of data management, protection, and security (even though it continued to accept and retain such fees), or take other steps to correct these flaws and vulnerabilities.

75. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and the Class members, because Defendants failed to implement data management and security measures that Plaintiff and the Class paid for.

76. Further, as a result of Defendants' conduct, Plaintiff and the Class members suffered actual damages including, the diminished value of the paid-for health care services received.

77. Plaintiff has no adequate remedy at law.

#### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff Kellie Lynn Case, individually and on behalf of the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, and

appointing Plaintiff Case as representative of the Class, and appointing her counsel as Class Counsel;

B. Declaring that Defendants' actions, as described above, constitute (i) Breach of Express Contract, (ii) Breach of Implied Contract (in the alternative to Breach of Express Contract), and (iii) Restitution/Unjust Enrichment (in the alternative to Breach of Express Contract and Breach of Implied Contract);

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including: (i) an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Defendants to protect all data collected through the course of their business in accordance with HIPAA, Fla. Stat. Ann. § 395.3025(4), and industry standards;

D. Awarding damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding restitution to Plaintiff and the Class in an amount to be determined at trial;

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

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

H. Awarding 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.

Respectfully submitted,

**KELLIE LYNN CASE**, individually and on behalf  
of all others similarly situated,

Dated: February 18, 2015

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

Edmund A. Normand  
ed@ednormand.com  
Florida Bar No. 865590  
Edmund A. Normand PLLC  
4381 New Broad Street  
Orlando, Florida 32814  
Tel: 407.625.9043

Ari J. Scharg\*  
ascharg@edelson.com  
EDELSON PC  
350 North LaSalle Street, Suite 1300  
Chicago, Illinois 60654  
Tel: 312.589.6370  
Fax: 312.589.6378

\* Admission *pro hac vice* be sought.