UNITED STATES DISTRICT COURT

MIDDLE DISTRICT OF FLORIDA

CHRYSTAL HOLMES, on behalf of herself and all others similarly situated, Plaintiff, v. THE VILLAGES TRI-COUNTY MEDICAL CENTER, INC. d/b/a UF HEALTH CENTRAL FLORIDA; LEESBURG REGIONAL MEDICAL CENTER, INC. d/b/a UF HEALTH CENTRAL FLORIDA; and CENTRAL FLORIDA HEALTH, INC. d/b/a UF HEALTH CENTRAL FLORIDA Defendants.	Case No.: **DEFENDANTS' NOTICE OF REMOVAL** [Filed concurrently with Civil Cover Sheet and Corporate Disclosure Statement] Action Filed: September 3, 2021 Complaint Served: September 15, 2021

TO THE CLERK OF THE ABOVE-ENTITLED COURT:

PLEASE TAKE NOTICE that pursuant to 28 U.S.C. §§ 1332(d), 1441, 1446, and 1453, Defendants The Villages Tri-County Medical Center, Inc. d/b/a UF Health Central Florida ("The Villages"); Leesburg Regional Medical Center, Inc. d/b/a UF Health Central Florida ("LRMC"); and UF Health Central Florida d/b/a UF Health Central Florida ("Central Florida") (collectively, "UF Health Central Florida" or "Defendants") removes the action filed by Chrystal Holmes ("Plaintiff"), on behalf of herself and all others similarly situated, in the Circuit Court for the Fifth

Judicial Circuit in and for Lake County, Florida, Case No. 35-2021-CA-001536-AXXX-XX, to the United States District Court for the Middle District of Florida.

JURISDICTION AND VENUE

1. This is a civil action over which this Court has original subject matter jurisdiction under 28 U.S.C. § 1332, and removal is proper under the Class Action Fairness Act of 2005 ("CAFA"), codified in pertinent part at 28 U.S.C. § 1332(d).

2. This Court is in the judicial district and division embracing the place where the state court case was brought and is pending. Thus, this Court is the proper district court to which this case should be removed. 28 U.S.C. §§ 1441(a), 1446(a).

THE ACTION & TIMELINESS OF REMOVAL

FACTUAL AND PROCEDURAL BACKGROUND

3. On September 3, 2021, Plaintiff, on behalf of herself and, purportedly, all others similarly situated, filed a Class Action Complaint (the "Complaint") against UF Health Central Florida in the Circuit Court for the Fifth Judicial Circuit in and for Lake County, Florida, Case No. 35-2021-CA-001536-AXXX-XX (the "State Court Action"). Plaintiff filed the Complaint as a putative class action. A true and correct copy of the Complaint in the State Court Action is attached hereto as **Exhibit A**.

4. On September 15, 2021, Plaintiff served UF Health Central Florida with copies of the Summons and Complaint via process server. True and correct copies of the Summons and Proofs of Service are attached hereto as **Exhibit B.**

5. A copy of the docket in the State Court Action is attached as **Exhibit C.**

6. Pursuant to 28 U.S.C. § 1446(a), all other process, pleadings, and orders that have been filed and served in the State Court Action are attached to this Notice of Removal as **Exhibit D**.

7. This removal is timely because UF Health Central Florida filed this removal within 30 days of being served with the Complaint. *See* 28 U.S.C. § 1446(b) (notice of removal shall be filed within 30 days of service); *Murphy Bros. v. Michetti Pipe Stringing, Inc.*, 526 U.S. 344, 348 (1999) (time period for removal begins when the defendant is served).

CAFA JURISDICTION

8. Basis of Original Jurisdiction. This Court has original jurisdiction over this action under CAFA (codified in pertinent part at 28 U.S.C. § 1332(d)). Section 1332(d) provides that a district court shall have original jurisdiction over a class action with one hundred (100) or more putative class members, in which the matter in controversy, in the aggregate, exceeds the sum or value of $5 million. Section 1332(d) further provides that, for original jurisdiction to exist, "any member

of a class of plaintiffs" must be a "citizen of a State different from any Defendant." 28 U.S.C. § 1332(d)(2)(A).

9. As set forth below, pursuant to 28 U.S.C. § 1332(d) and § 1441(a), UF Health Central Florida may remove the State Court Action to federal court under CAFA because: (i) this action is pled as a class action; (ii) the putative class includes more than one hundred (100) members; (iii) members of the putative class are citizens of a state different from that of Defendants; and (iv) the matter in controversy, in the aggregate, exceeds the sum or value of $5,000,000, exclusive of interest and costs.

THE ACTION IS PLED AS A CLASS ACTION

10. CAFA defines a "class action" as "any civil action filed under rule 23 of the Federal Rules of Civil Procedure ***or similar State statute*** or rule of judicial procedure authorizing an action to be brought by 1 or more representative persons as a class action." 28 U.S.C. § 1332(d)(1)(B) (emphasis added).

11. Plaintiff brings this action as a "class action" and seeks class certification under Florida law pursuant to Florida Rules of Civil Procedure, Rule 1.220(b)(2), (b)(3), and (d)(4). [Compl. ¶¶ 1, 77.] Because "Florida's Class Action rule, Florida Rule of Civil Procedure 1.220, is based on Federal Rule of Civil Procedure 23," *Concerned Class Members v. Sailfish Point, Inc.*, 704 So. 2d 200,

201 (Fla. Dist. Ct. App. 1998), the first CAFA requirement is met. [Compl., ¶ 77 ("Plaintiff brings this nationwide class action . . .").]

THE PUTATIVE CLASS INCLUDES AT LEAST ONE HUNDRED (100) MEMBERS

12. Plaintiff alleges that "[o]n or around May 29 to May 31, 2021, an unauthorized actor obtained unauthorized access to [Defendants'] computer network as part of a ransomware attack" that may have resulted in the unauthorized actor accessing the "PII and PHI of [Defendants'] current and former patients…" (the "Ransomware Attack").[1] [Compl., ¶¶ 5-6.] Plaintiff further alleges that the Ransomware Attack occurred as a result of Defendants' "failure to: (i) adequately protect the PII and PHI of [Defendants'] current and former patients; (ii) warn [Defendants'] current and former patients of [Defendants'] inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents." [Compl., ¶ 12.]

[1] Plaintiff defines "PII" as "names, addresses, dates of birth, and/or Social Security numbers." [Compl., ¶ 1.] Plaintiff defines "PHI" as "health insurance information, medical record numbers, patient account numbers, and/or limited treatment information." [*Id*.]

13. Based on these allegations, Plaintiff asserts three causes of action against Defendants: (1) negligence, (2) breach of contract, and (3) breach of fiduciary duty. [*See, generally,* Compl.]

14. Furthermore, Plaintiff purports to bring these three causes of action on behalf of herself and a nationwide class (the "Class"). [Compl., ¶ 78.] Plaintiff defines the Class as: "All individuals whose PII and/or PHI was accessed or potentially accessed during the [Ransomware Attack] event referenced in the Website Notice." [*Id.*]

15. Although Plaintiff alleges that "the exact numbers of members in the Class can be ascertained through Defendants' records," she does allege that "[o]n July 30, 2021, Defendants notified the U.S. Department of Health and Human Services that 700,981 individuals were affected by the [Ransomware Attack]." [Compl., ¶ 81.]

16. Defendants mailed notification to approximately 646,358 people within the United States that their information may have been impacted by the Ransomware Attack.

17. Therefore, the number of putative class members exceeds the statutorily required minimum of 100.

MINIMAL DIVERSITY OF CITIZENSHIP EXISTS

18. Pursuant to 28 U.S.C. § 1332(d)(2)(A), the "district court shall have original jurisdiction" over a "class in which . . . any member of the class of plaintiffs is a citizen of a State different from any defendant." (emphasis added). *See also Day v. Sarasota Drs. Hosp., Inc.*, No. 8:19-CV-1522-T-33TGW, 2020 WL 5758003, at *2 (M.D. Fla. Sept. 28, 2020) (stating that minimal diversity is met if "a single putative class member was a citizen of a state other than [that of Defendants] at the time of removal").

19. Plaintiff's and the Putative Class' Citizenship. To be a "citizen" of a state, the individual must not only reside in that state, but he or she also must "inten[d] to remain in that state." *Smith v. Marcus & Millichap, Inc.*, 991 F.3d 1145, 1157 (11th Cir. 2021). Here, Plaintiff alleges in the Complaint that she "is a citizen of Florida residing in Lake County, Florida." [Compl., ¶ 15.] The putative class she seeks to represent, however, is much broader and more expansive geographically. After determining whose information could have potentially been impacted by the Ransomware Attack, Defendants sent notifications of the Ransomware Attack to people with addresses in all 50 states and the District of Columbia. And while "residency does not equate to citizenship," *Smith*, 991 F.3d at 1157 (11th Cir. 2021), in this case, where only one putative class member must reside and intend to remain

in a state different than Florida, it is more likely than not that at least one of the approximately 646,358 putative class members is a non-Florida citizen.

20. Defendants' Citizenship. Pursuant to 28 U.S.C. § 1332(c), "a corporation shall be deemed to be a citizen of any State by which it has been incorporated and of the State where it has its principal place of business." The United States Supreme Court has concluded that a corporation's "principal place of business" is "where a corporation's officers direct, control, and coordinate the corporation's activities," *i.e.*, the corporation's "nerve center." *Hertz Corp. v. Friend*, 130 S. Ct. 1181, 1192 (2010). "[I]n practice," a corporation's "nerve center" should "normally be the place where the corporation maintains its headquarters." *Id*. "The public often (though not always) considers it the corporation's main place of business." *Id*. at 1193.

21. The Villages is a Florida corporation.

22. Pursuant to *Hertz*'s nerve center test, The Villages has its principal place of business in Florida. Specifically, its headquarters are located at 1451 El Camino Real, The Village, Fl 32159. Accordingly, The Villages is a citizen of the State of Florida.

23. LRMC is a Florida Corporation.

24. Pursuant to *Hertz*'s nerve center test, LRMC has its principal place of business in Florida. Specifically, its headquarters are located at 600 E. Dixie

Avenue, Leesburg, FL 34748. Accordingly, LRMC is a citizen of the State of Florida.

25. Central Florida is a Florida corporation.

26. Pursuant to *Hertz*'s nerve center test, Central Florida has its principal place of business in Florida. Specifically, its headquarters are located at 410 Childs St., Leesburg, FL, 34748. Accordingly, Central Florida is a citizen of the State of Florida.

27. As established in Paragraphs 20-26 above, minimal diversity of citizenship exists pursuant to CAFA because each of the Defendants is a citizen of the State of Florida, and it is more likely than not that at least one of the approximately 646,358 putative class members is a citizen of a state other than Florida.

28. Furthermore, neither Defendants nor Plaintiff can show, let alone demonstrate, that CAFA's "local controversy exception" applies. The "local controversy exception" requires a district court to "decline to exercise jurisdiction when three requirements are met: (1) greater than two-thirds of the proposed plaintiff class are citizens of the state of filing; (2) at least one 'significant defendant' is a citizen of the state of filing; and (3) the principal injuries were incurred in the state of filing." *Smith.*, 991 F.3d at 1155 (citing 28 U.S.C. § 1332(d)(4)(A)(i)). With over 640,000 putative class members with addresses in all 50 states, there simply is no

way to know who is a citizen of what state without speaking directly to each of those over 640,000 individuals. *Smith*, 991 F.3d at 1157 (holding that to prove "citizenship" for the purpose of the local controversy exception, the plaintiff "must provide evidence of the class members' state of residence as well as evidence showing their intent to remain in that state" and that "[m]ere mental fixing of citizenship is not sufficient. What is in another man's mind must be determined by what he does as well as by what he says"). This is especially true here, where "citizens of other states may live part of the year in Florida…, but maintain a permanent residence elsewhere." *Id* at 1158. Further exacerbating this problem is the nature of the putative class here, many of whom were residents in nursing care facilities. And, as the Court in *Smith* noted, just because a person "ha[s] to enter into a short-term care nursing facility while in Florida" in no way means they are citizens of Florida. *Id*.

THE AMOUNT IN CONTROVERSY EXCEEDS THE CAFA THRESHOLD[2]

29. Where a complaint does not specify the amount of damages sought, as is the case with Plaintiff's Complaint, the removing defendants must prove by a

[2] The amounts set forth in this Notice of Removal are solely for purposes of establishing that the amount in controversy exceeds the $5,000,000 threshold and are not intended and cannot be construed as an admission that Plaintiff can state a claim or is entitled to damages in any amount. Defendants deny liability, deny

preponderance of the evidence that the jurisdictional amount-in-controversy is satisfied. 28 U.S.C.A. § 1446(c)(2)(B). The United States Supreme Court has held that "a defendant's notice of removal need include only a plausible allegation that the amount in controversy exceeds the jurisdictional threshold" to meet the amount-in-controversy requirement. *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 90 (2014).

30. As demonstrated below, the allegations in the Complaint make it more likely than not that the amount in controversy under CAFA exceeds $5,000,000.

31. Breach-of-Contract Claim. Plaintiff alleges that "Defendants acquired and maintained the PII and PHI of Plaintiff and the…Class" and that, in doing so, "entered into contracts with Plaintiff and the…Class requiring Defendants to protect and keep private medical information of Plaintiff and the…Class." [Compl., ¶¶ 130, 132.] Plaintiff further alleges that "Defendants breached the contract they made with Plaintiff and the…Class by failing to protect and keep private medical information of Plaintiff and the…Class." [Compl., ¶ 134.]

32. As a result of Defendants' alleged breach of contract, Plaintiff claims that she and the Class "have suffered (and will continue to suffer) ongoing,

---

Plaintiff is entitled to recover any amount, and deny that a class can be properly certified in this matter.

imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of confidentiality of the stolen data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm." [Compl., ¶ 135.]

33. Plaintiff's Complaint contains no allegations that would support or suggest the amount in actual damages to which she or any of member of the Class are allegedly entitled for Defendants' alleged breach of contract. However, because Plaintiff does seek recovery for time and money spent "scrutinizing bank statements, credit card statements, and credit reports," as well as "expenses and/or time spent initiating fraud alerts [and] decreased credit scores and ratings," one option for assigning a value to these damages is through the cost of credit monitoring. The cost of credit monitoring is the "out-of-pocket expenses" associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or authorized use of their PII and PHI that Plaintiff alleges she and the Class are at risk of in the future.

34. Three main identity-protection agencies—Equifax, LifeLock, and Experian—advertise monthly rates for credit-monitoring services ranging from

$14.99 to $19.95 per person per month. For example, LifeLock offers a product, titled Norton360 with LifeLock, that provides 1-Bureau credit monitoring with up to $25,000 in "stolen funds reimbursement" for $14.99 per month.[3] Similarly, both Equifax[4] and Experian[5] offer products that provide 3-Bureau credit monitoring with up to $1 million in identity theft insurance for $19.95 per month. Multiplying just the cost of providing one month of credit-monitoring services at $14.99 (the cheapest

---

[3] *See* https://www.lifelock.com/family-plans/?promocode=BSEM60MBGCBU&om_sem_cid=hho_sem_sy:us:ggl:en:e:br:ll&utm_source=google&utm_medium=cpc&utm_campaign=1584904959&adgroup=66661422904&utm_term=lifelock%2520credit%2520monitoring&targetid=kwd-295997165667&matchtype=e&utm_content=297610135624&network=g&device=c&adp=&testgroup=&pgrid=66661422904&ptaid=kwd-295997165667&gclid=EAIaIQobChMI0v-3-eG28wIVEFpgCh2XSQzTEAAYASABEgLMPPD_BwE&gclsrc=aw.ds (last visited: October 6, 2021).

[4] *See* https://www.equifax.com/equifax-complete/Equifax/?CID=2_equifax%20credit%20monitoring_G_e&adID=502355994880&DS3_KIDS=p50281164756&campaignid=71700000061086345&sakwid=43700050281164756&gclid=EAIaIQobChMIzpzAneG28wIVS9KzCh3vCA_MEAAYASAAEgIjevD_BwE&gclsrc=aw.ds (last visited: October 6, 2021)

[5] See https://www.experian.com/lp/creditlock.html?bcd=ad_c_sem_427_515842009606&k_id=_k_EAIaIQobChMIzZ63geO28wIVTR-tBh0rgAUsEAAYASABEgIWwfD_BwE_k_&k_kw=aud-422897489015:kwd-317312162328&k_mt=e&pc=sem_exp_google&cc=sem_exp_google_ad_858684474_43905679139_515842009606_aud-422897489015:kwd-317312162328_e___k_EAIaIQobChMIzZ63geO28wIVTR-tBh0rgAUsEAAYASABEgIWwfD_BwE_k_&ref=identity&awsearchcpc=1&gclid=EAIaIQobChMIzZ63geO28wIVTR-tBh0rgAUsEAAYASABEgIWwfD_BwE (last visited: October 6, 2021).

of the three products) by the number of putative class members, the amount in controversy for just credit monitoring is approximately $9,688,906.42 (calculated as: 646,358 individuals notified, times 1 month, times $14.99 per month).

35. Negligence Claim. Plaintiff alleges that Defendants, "through their actions and/or omissions, unlawfully breached [their] duties to Plaintiff and the…Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the…Class during the time the PII and PHI was within Defendant's possession and control." [Compl., ¶ 111.] Specifically, Plaintiff alleges (1) that "[a]s a condition of their treatment by Defendants, Defendants' current and former patients were obligated to provide and entrust Defendants with certain PII and PHI" [Compl., ¶ 94]; (2) that "Plaintiff and the…Class entrusted their PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties" [Compl., ¶ 95]; (3) that "Defendants had a duty to," among other things, "exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties" [Compl., ¶ 98]; and (4) that Defendants breached that duty [Compl., ¶ 111].

36. Plaintiff further alleges that "[a]s a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the…Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or authorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity address and attempting to mitigate the present and future consequences of the [Ransomware Attack], including, but not limited to, efforts spent researching how to prevent, detect, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk of their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the current and former patients' PII and PHI in their continued possessions; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the [Ransomware Attack] for the remained of the lives of Plaintiff and the Class." [Compl., 124.]

37. Plaintiff's Complaint contains no allegations that would support or suggest the amount in actual damages to which she or any of member of the Class

are allegedly entitled for Defendants' alleged breach of contract. But, as stated above, just one month of Norton360 with LifeLock for each member of the Class would amount to, at a minimum, $9,688,906.42. Plaintiff's other allegations do not support or suggest the amount in other economic and noneconomic damages, especially given that Plaintiff does not allege that either she or any member of the Class has suffered fraud, attempted fraud, or out-of-pocket expenses as a result of the Ransomware Attack. Therefore, Defendants do not include in the calculation of the total amount in controversy Plaintiff's alleged damages arising from Defendants' alleged negligent acts or omissions. However, when these alleged damages are combined with the cost of just one month of credit monitoring for the entire Class, the amount in controversy further exceeds CAFA's $5,000,000 threshold.[6]

38. Breach-of-Fiduciary-Duty Claim. Plaintiff alleges that "a relationship existed between [her], the…Class, and Defendants in which [she] and the…Class put their trust in Defendants to protect the private information of Plaintiff and the…Class and Defendants accepted that trust." [Compl., ¶ 139.] Plaintiff further alleges that Defendants "breached that fiduciary duty…by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest

[6] As discussed below in Paragraphs 42 and 43, to the extent Plaintiff can recover any money under either her negligence or breach-of-confidence claims, that amount is capped at $300,000 pursuant to Florida's sovereign immunity statute.

loyalty, and failing to protect the private information of Plaintiff and the…Class." [Compl., ¶ 140.]

39. Plaintiff alleges that "[a]s a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff [is] entitled to and demand[s] actual, consequential, and nominal damages and injunctive relief." [Compl., ¶ 144.] Plaintiff's Complaint, however, contains no allegations that would support or suggest the amount in "actual, consequential, and nominal damages" she or any member of the Class allegedly sustained as a result of Defendants' alleged breach of fiduciary duty. Therefore, Defendants do not include in the calculation of the total amount in controversy Plaintiff's or the Class' alleged breach-of-fiduciary-duty damages. However, when Plaintiff's and the Class' alleged breach-of-fiduciary-duty damages are combined with the cost of just one month of Norton360 with LifeLock credit monitoring for each member of the Cass, the amount in controversy further exceeds CAFA's $5,000,000 threshold.

40. Total Amount in Controversy. Based on the discussion above, the amount in controversy based just on one month of Norton360 with LifeLock credit monitoring for each member of the Cass exceeds the $5,000,000 CAFA minimum before ever taking into account other forms of compensatory damages, injunctive relief, or attorneys' fees, which, as discussed below, adds even more to the total amount in controversy.

41. Other Claims. In addition to the damages discussed above, Plaintiff also requests injunctive relief for herself and the Class. [Compl., Prayer for Relief.] In certain circumstances, where the value of injunctive relief is not too speculative, the value can be considered when determining the amount in controversy. *Anderson v. Wilco Life Ins. Co.*, 943 F.3d 917, 929 (11th Cir. 2019) (finding CAFA jurisdiction where the plaintiffs' "injunctive demand…is an integral and key component of her complaint valued at over $75 million."). Here, however, no allegations in the Complaint allow Defendants to calculate the amount of Plaintiff's injunctive relief demand, and, therefore, Defendants have not included that value in the calculation o of the total amount in controversy. Nevertheless, Defendants underscore the allegations to the Court as further evidence that the amount in controversy exceeds $5,000,000, as already established above.

IMPACT OF IMMUNITY

42. Under well-settled Florida law, the state and its agencies or subdivisions are entitled to sovereign immunity. *See* Fla. Stat. Ann.§ 768.28(1). Under that statute, "[a]ctions at law against the state or any of its agencies or subdivisions to recover damages in tort for money damages against the state or its agencies or subdivisions for injury or loss of property, personal injury, or death caused by the negligent or wrongful act or omission of any employee of the agency or subdivision while acting within the scope of the employee's office or employment

under circumstances in which the state or such agency or subdivision, if a private person, would be liable to the claimant, in accordance with the general laws of this state, may be prosecuted ***subject to the limitations specified in this act***." *Id.* (emphasis added). More specifically, "[n]either the state nor its agencies or subdivisions shall be liable to pay a claim or a judgment by any one person which exceeds the sum of $200,000 or any claim or judgment, or portions thereof, which, when totaled with all other claims or judgments paid by the state or its agencies or subdivisions arising out of the same incident or occurrence, exceeds the sum of $300,000." *Id.* at § 768.28(5)(a). Defendants are "not-for-profit subsidiary[ies]" of Shands Teaching Hospital and Clinics, Inc., and, therefore, any recovery for tort claims against Defendants is unquestionably capped at $300,000. Fla. Stat. Ann. § 1004.41 (4)(e).

43. Defendants also believe that sovereign immunity bars entirely Plaintiff from recovering under her breach-of-contract claim. However, based on Defendants' meet-and-confer efforts with Plaintiff, Defendant understands that Plaintiff does not believe sovereign immunity has any impact on her breach-of-contract claim. Thus, while any amounts Plaintiff may recover under her two tort claims will be capped at $300,000, Plaintiff has alleged, as discussed above, more than $5,000,000 in controversy for her breach-of-contract claim, should it survive at all.

NOTICE

44. As required by 28 U.S.C. § 1446(d), Defendants are providing written notice of the filing of this Notice of Removal to Plaintiff and are filing a copy of this Notice of Removal with the Clerk of the Circuit Court for the Fifth Judicial Circuit in and for Lake County, Florida.

Respectfully submitted,

DATED: October 14, 2021

BAKER & HOSTETLER LLP

By: */s/ Julie Singer Brady*

Julie Singer Brady
Florida Bar No. 389315
Email: *jsingerbrady@bakerlaw.com*
200 South Orange Avenue, Suite 2300
Orlando, FL 32801
Telephone: 407.649.4000
Facsimile: 407.841.0168

Attorneys for Defendants
THE VILLAGES TRI-COUNTY MEDICAL CENTER, INC. d/b/a UF HEALTH CENTRAL FLORIDA; LEESBURG REGIONAL MEDICAL CENTER, INC. d/b/a UF HEALTH CENTRAL FLORIDA; and CENTRAL FLORIDA HEALTH, INC. d/b/a UF HEALTH CENTRAL FLORIDA

CERTIFICATE OF SERVICE

I certify that a true and correct copy of the foregoing **DEFENDANTS' NOTICE OF REMOVAL** was filed and served through the Court's ECF system on this 14th day of October, 2021, on all counsel of record.

/s/ Julie Singer Brady
Julie Singer Brady

Exhibit A
to
Notice of Removal

Filing # 134054313 E-Filed 09/03/2021 05:30:50 PM

IN THE CIRCUIT COURT FOR THE FIFTH JUDICIAL CIRCUIT IN AND FOR LAKE COUNTY, FLORIDA

CHRYSTAL HOLMES, on behalf of herself and all others similarly situated, Plaintiff, vs. THE VILLAGES TRI-COUNTY MEDICAL CENTER, INC. d/b/a UF HEALTH CENTRAL FLORIDA, LEESBURG REGIONAL MEDICAL CENTER, INC. d/b/a UF HEALTH CENTRAL FLORIDA, and CENTRAL FLORIDA HEALTH, INC. d/b/a UF HEALTH CENTRAL FLORIDA, Defendants.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Chrystal Holmes ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against The Villages Tri-County Medical Center, Inc. d/b/a UF Health Central Florida, Leesburg Regional Medical Center, Inc. d/b/a UF Health Central Florida ("Leesburg Hospital"), and Central Florida Health, Inc. d/b/a UF Health Central Florida (collectively, "Defendants"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personal identifiable information that they acquired from their patients. Defendants required this information from their patients or recorded this information for their

patients as a condition or result of medical treatment, including without limitation, names, addresses, dates of birth, and/or Social Security numbers (collectively, "personal identifiable information" or "PII") as well as health insurance information, medical record numbers, patient account numbers, and/or limited treatment information (collectively, "protected health information" or "PHI").

2. Defendants are the registered owners of the fictious name "UF Health Central Florida" ("UFHCF") and individually and collectively operate under this fictitious name.

3. UFHCF is a health care system that "care[s] for patients in Lake, Sumter, and Marion counties through inpatient acute hospital services at UF Health The Villages® Hospital and UF Health Leesburg Hospital, inpatient rehabilitation services at UF Health The Villages® Rehabilitation Hospital, adult inpatient psychiatric services at the UF Health Leesburg Hospital Senior Behavioral Health Center and diagnostic laboratory services at several locations."[1]

4. In order to obtain medical treatment, Plaintiff and other patients of UFHCF entrust and provide to UFHCF an extensive amount of PII. UFHCF also records an extensive amount of PHI regarding its patients, including treatment information. UFHCF retains this information on computer hardware—even long after the treatment relationship ends. UFHCF acknowledges that it understands the importance of protecting information.

5. On or around May 29 to May 31, 2021, an unauthorized actor obtained unauthorized access to UFHCF's computer network as part of a ransomware attack (the "Cybersecurity Event").

6. The unauthorized actor may have accessed the PII and PHI of UFHCF's current and former patients, including Plaintiff and Class Members.

[1] *See* "About Us", https://www.centralfloridahealth.org/ (last visited Aug. 30, 2021).

7. In a "Notice to Our Patients of Cybersecurity Event" posted on its website (the "Website Notice"), UFHCF advised that it was informing its current and former patients of the Cybersecurity Event and mailing them letters.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, UFHCF assumed legal and equitable duties to those individuals. UFHCF admits that the unencrypted PII and PHI exposed to "unauthorized activity" included names, addresses, dates of birth, and/or Social Security numbers as well as health insurance information, medical record numbers, patient account numbers, and/or limited treatment information.

9. The exposed PII and PHI of UFHCF's current and former patients can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. UFHCF's current and former patients face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

10. This PII and PHI was compromised due to UFHCF's negligent and/or careless acts and omissions and the failure to protect PII and PHI of UFHCF's current and former patients.

11. Until notified of the breach, Plaintiff and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

12. Plaintiff bring this action on behalf of all persons whose PII and/or PHI was compromised as a result of UFHCF's failure to: (i) adequately protect the PII and PHI of UFHCF's current and former patients; (ii) warn UFHCF's current and former patients of UFHCF's inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities

and incidents. UFHCF's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of UFHCF's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Cybersecurity Event, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in UFHCF's possession and is subject to further unauthorized disclosures so long as UFHCF fails to undertake appropriate and adequate measures to protect the PII and PHI, and at the very least, are entitled to nominal damages .

14. UFHCF disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that UFHCF's current and former patients' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

15. Plaintiff Chrystal Holmes is a citizen of Florida residing in Lake County, Florida. On or around July 30, 2021, Plaintiff Holmes received UFHCF's letter notifying her of the

Cybersecurity Event.

16. Defendant The Villages Tri-County Medical Center, Inc. d/b/a UF Health Central Florida is a corporation organized under the laws of Florida, headquartered at 1451 El Camino Real, The Villages, FL, with its principal place of business in The Villages, FL.

17. Defendant Leesburg Regional Medical Center, Inc. d/b/a UF Health Central Florida is a corporation organized under the laws of Florida, headquartered at 600 E. Dixie Avenue, Leesburg, FL, with its principal place of business in Leesburg, FL.

18. Defendant Central Florida Health, Inc. d/b/a UF Health Central Florida is a corporation organized under the laws of Florida, headquartered at 410 Childs St., Leesburg, FL, with its principal place of business in Leesburg, FL.

19. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

20. All of Plaintiff's claims stated herein are asserted against UFHCF and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

21. The Court has subject matter jurisdiction over Plaintiff's claims under Florida Stat. § 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages in excess of $30,000.00 dollars, exclusive of interest and attorneys' fees.

22. The Court has personal jurisdiction over Defendants under Florida Stat. § 48.193, because Defendants personally or through their agents operated, conducted, engaged in, or carried on a business or business venture in Florida; had offices in Florida; committed tortious acts in

Florida; and/or breached a contract in Florida by failing to perform acts required by the contract to be performed in Florida.

23. Venue is proper in Lake County pursuant to Florida Stat. § 47.011 and § 47.051 because Defendants are headquartered and do business in Lake County, the cause of action accrued in Lake County, and/or Defendants have offices for the transaction of their customary business in Lake County.

IV. FACTUAL ALLEGATIONS

Background

24. UFHCF operates dozens of medical facilities throughout Florida under a variety of fictitious names, including AdventHealth Medical Group Surgical Specialists at Tampa.

25. Plaintiff and Class Members treated by UFHCF were required to provide some of their most sensitive and confidential information, including names, addresses, dates of birth, and/or Social Security numbers as well as health insurance information, medical record numbers, patient account numbers, and/or limited treatment information. This information is static, does not change, and can be used to commit myriad financial crimes.

26. In providing treatment to Plaintiff and Class Members, UFHCF generated and retained additional sensitive personal information about Plaintiff and Class Members, including medications lists and clinical documentation/notes.

27. Plaintiff and Class Members, as current and former patients, relied on UFHCF to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. UFHCF's current and former patients demand security to safeguard their PII and PHI.

28. UFHCF had a duty to adopt reasonable measures to protect Plaintiff's and Class

Members' PII and PHI from involuntary disclosure to third parties.

The Cybersecurity Event

29. Defendant Leesburg Hospital posted a "Privacy policy" on its website (the "Privacy Notice"), effective April 14, 2003 and revised February 17, 2010 and September 23, 2013.[2]

30. The Private Notice states that "[a]ll of the UF Health Central Florida's entities, sites and locations follow the terms of this notice, including but not limited to: UF Health Leesburg Hospital, UF Health The Villages® Hospital, UF Health The Villages® Hospital Rehabilitation Hospital, UF Health Leesburg Hospital Urgent Care Center, UF Health Alliance Laboratory, and all other affiliated sites and locations."[3]

31. The Privacy Notice states "[w]e understand that medical information about you and your health is personal. We are committed to protecting that medical information."[4]

32. The Privacy Notice states "[w]e are required by law to make sure that health-related information that identifies you is kept private."[5]

33. Prior to the Cybersecurity Event, UFHCF should have (i) encrypted or tokenized the sensitive PII and PHI of Plaintiff and the Nationwide Class, (ii) deleted such PII and PHI that it no longer had reason to maintain, (iii) eliminated the potential accessibility of the PII and PHI from the Internet, and (iv) otherwise reviewed and improved the security of its computer system.

34. Prior to the Cybersecurity Event, UFHCF did not (i) encrypt or tokenize the sensitive PII and PHI of Plaintiff and the Nationwide Class, (ii) delete such PII and PHI that it no

---

[2] Ex. 1, *available at* https://www.leesburgregional.org/privacy-policy/ (last visited August 30, 2021).

[3] *Id.*

[4] *Id.*

[5] *Id.*

longer had reason to maintain, (iii) eliminate the potential accessibility of the PII and PHI from the Internet, and (iv) otherwise review and improve the security of its computer system.

35. On or around July 30, 2021, UFHCF posted the Website Notice.[6] The Website Notice provided, in part, as follows:

> On May 31, 2021, UF Health Central Florida — including UF Health Leesburg Hospital and UF Health The Villages® Hospital — detected unusual activity involving its computer systems. We took immediate action to contain the event, including reporting it to law enforcement and launching an investigation with independent experts. UF Health's Gainesville or Jacksonville campuses were not affected.
>
> The investigation determined that unauthorized access to UF Health Central Florida's computer network occurred between May 29 and May 31, 2021. During this brief time period, some patient information may have been accessible, such as names, addresses, dates of birth, Social Security numbers, health insurance information, medical record numbers and patient account numbers, as well as limited treatment information used by UF Health for its business operations. UF Health's electronic medical records were not involved or accessed.
>
> We have no reason to believe the information was further used or disclosed; however, on July 30, 2021, we began mailing letters to individuals whose data may have been involved and, as a precautionary measure, are offering them complimentary credit monitoring and identity protection services. Patients are also encouraged to review statements from their health insurer, and to contact them immediately if they see any services they did not receive. We also established a dedicated call center for patients to call with questions. If you believe you are affected, but do not receive a letter by Aug. 16, 2021, please call 1-833-909-3926 between 9 a.m. and 9 p.m. Eastern Time Monday through Friday.[7]

36. UFHCF admitted in the Website Notice that unauthorized third persons may have

---

[6] Ex. 2, available at https://www.leesburgregional.org/notice-to-our-patients-of-cybersecurity-event/ (last visited Aug. 30, 2021).

[7] *Id.* at 1.

accessed sensitive information about current and former patients of UFHCF, including names, addresses, dates of birth, and/or Social Security numbers as well as health insurance information, medical record numbers, patient account numbers, and/or limited treatment information.

37. Plaintiff's and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of the affected current and former patients. Unauthorized individuals can easily access the PII and PHI of UFHCF's current and former patients.

38. UFHCF did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former patients, causing the exposure of PII and PHI for more than 700,000 individuals.

39. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

40. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Cybersecurity Event, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Mar. 15, 2021).

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

41. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Cybersecurity Event, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are

[9] *Id.* at 3-4.

the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[10]

42. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Cybersecurity Event, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

[10] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Mar. 15, 2021).

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[11]

43. Given that Defendants were storing the PII and PHI of more than 700,000 individuals, Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

44. The occurrence of the Cybersecurity Event indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting

[11] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Mar. 15, 2021).

in the Cybersecurity Event and the exposure of the PII and PHI of more than 700,000 individuals, including Plaintiff and Class Members.

UFHCF Acquires, Collects and Stores Plaintiff's and Class Members' PII and PHI.

45. UFHCF acquired, collected, and stored UFHCF's current and former patients' PII and PHI.

46. As a condition of maintaining treatment with UFHCF, UFHCF requires that its patients entrust UFHCF with highly confidential PII and PHI.

47. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, UFHCF assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII and PHI from disclosure.

48. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI. Plaintiff and the Class Members, as current and former patients, relied on the UFHCF to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

49. UFHCF could have prevented this Cybersecurity Event by properly securing and encrypting Plaintiff's and Class Members' PII and PHI, or UFHCF could have destroyed the data, especially old data from former patients that UFHCF had no legal right to retain.

50. UFHCF's negligence in safeguarding UFHCF's current and former patients' PII and PHI is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

51. Despite the prevalence of public announcements of data breach and data security

compromises, UFHCF failed to take appropriate steps to protect the PII and PHI of Plaintiff and the proposed Class from being compromised.

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

53. The ramifications of UFHCF's failure to keep secure UFHCF's current and former patients' PII and PHI are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information and Protected Health Information

54. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or

[12] 17 C.F.R. § 248.201 (2013).

[13] *Id.*

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2021).

debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

55. Social Security numbers, for example, are among the mot sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

56. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

57. Even then, a new Social Security number may not be effective. According to Julie

---

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2021).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Jan. 26, 2021).

[17] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2021).

Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

58. Based on the foregoing, the information compromised in the Cybersecurity Event is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Cybersecurity Event is impossible to "close" and difficult, if not impossible, to change—name, address, date of birth, and Social Security number.

59. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19]

60. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

61. The PII and PHI of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to others criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Cybersecurity Event may not come to light for years.

---

[18] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 26, 2021).

[19] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2021).

62. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

63. At all relevant times, UFHCF knew, or reasonably should have known, of the importance of safeguarding UFHCF's current and former patients' PII and PHI, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if UFHCF's data security system was breached, including, specifically, the significant costs that would be imposed on UFHCF's current and former patients as a result of a breach.

64. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

65. UFHCF was, or should have been, fully aware of the unique type and the significant volume of data on UFHCF's network, amounting to potentially thousands of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

66. Although UFHCF has offered its current and former patients credit monitoring and identity protection services, the offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at

---

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed Jan. 26, 2021).

issue here.

67. The injuries to Plaintiff and Class Members were directly and proximately caused by UFHCF's failure to implement or maintain adequate data security measures for the PII and PHI of UFHCF's current and former patients.

Plaintiff Holmes's Experience

68. In 2020 and/or 2021, Plaintiff Holmes was a patient of Defendant Leesburg Hospital. As a condition for treatment, she was required to provide and entrust her PII and PHI, including but not limited to her name, address, date of birth, and/or Social Security number as well as health insurance information, medical record number, patient account number, and/or limited treatment information.

69. On or around July 30, 2021, Plaintiff Holmes received a letter notifying her of the Cybersecurity Event.

70. As a result of the letter notifying her of the Cybersecurity Event, Plaintiff Holmes spent time dealing with the consequences of the Cybersecurity Event, which includes time spent verifying the legitimacy of the letter, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

71. Additionally, Plaintiff Holmes is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

72. Plaintiff Holmes stores any documents containing her PII and PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

73. Plaintiff Holmes suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Holmes entrusted to UFHCF for the purpose of her treatment, which was compromised in and as a result of the Cybersecurity Event.

74. Plaintiff Holmes suffered lost time, annoyance, interference, and inconvenience as a result of the Cybersecurity Event and has anxiety and increased concerns for the loss of her privacy.

75. Plaintiff Holmes has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, especially her Social Security number, in combination with her name and date of birth, being placed in the hands of unauthorized third-parties and possibly criminals.

76. Plaintiff Holmes has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in UFHCF's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

77. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 1.220(b)(2), (b)(3), and (d)(4) of the Florida Rules of Civil Procedure.

78. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose PII and/or PHI was accessed or potentially accessed during the cybersecurity event referenced in the Website Notice (the "Nationwide Class").

79. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

80. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

81. Numerosity, Fla R. Civ. P. 1.220(a)(1): The Nationwide Class (the "Class") is so numerous that joinder of all members is impracticable. On July 30, 2021, Defendants notified the U.S. Department of Health and Human Services Office for Civil Rights that 700,981 individuals were affected by the Cybersecurity Event. In any event the exact numbers of members in the Class can be ascertained through Defendants' records.

82. Commonality, Fla. R. Civ. P. 1.220(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendants had respective duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had a duty not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Cybersecurity Event;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cybersecurity Event;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Cybersecurity Event to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Cybersecurity Event.

83. Typicality, Fla. R. Civ. P. 1.220(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Cybersecurity Event, due to Defendants' misfeasance.

84. 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 Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members 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.

85. Adequacy, Fla. R. Civ. P.1.220(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

86. Superiority and Manageability, Fla. R. Civ. P. 1.220(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

87. The nature of this action and the nature of laws available to Plaintiff and Class

Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

88. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

89. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

90. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII and PHI of Class Members and Defendants may continue to act unlawfully as set forth in this Complaint.

91. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 1.220(b)(2) of the Florida Rules of Civil Procedure.

92. Likewise, particular issues under Rule 1.220(d)(4) are appropriate for certification

because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether UF Defendants HCF breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether a contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

e. Whether Defendants breached the contract;

f. Whether Defendants adequately, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cybersecurity Event;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

93. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

94. As a condition of their treatment by Defendants, Defendants' current and former patients were obligated to provide and entrust Defendants with certain PII and PHI, including their names, addresses, dates of birth, and/or Social Security numbers as well as health insurance information, medical record numbers, patient account numbers, and/or limited treatment information.

95. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

96. Defendants have full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII and/or PHI were wrongfully disclosed.

97. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former patients' PII and PHI involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

98. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing

Defendants' security protocols to ensure that Plaintiff's and the Nationwide Class's information in Defendants' possession was adequately secured and protected.

99. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former patients' PII and PHI it was no longer required to retain pursuant to regulations.

100. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Nationwide Class's PII and PHI.

101. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendants with their confidential PII and PHI, a necessary part of obtaining treatment from Defendants.

102. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff and the Nationwide Class.

103. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

104. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendants' systems.

105. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Cybersecurity Event as set forth herein. Defendants'

misconduct also included their decision not to comply with industry standards for the safekeeping of Plaintiff's and the Nationwide Class's PII, including basic encryption techniques freely available to Defendants.

106. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

107. Defendants was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Cybersecurity Event.

108. Defendants had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

109. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

110. Defendants have admitted that the PII and PHI of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Cybersecurity Event.

111. Defendants, through their actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide Class during the time the PII and PHI was within Defendants' possession or control.

112. Defendants improperly and inadequately safeguarded the PII and PHI of Plaintiff

and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Cybersecurity Event.

113. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect their current and former patients' PII and PHI in the face of increased risk of theft.

114. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former patients' PII and PHI.

115. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove former patients' PII and PHI it was no longer required to retain pursuant to regulations.

116. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Cybersecurity Event.

117. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been compromised.

118. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Nationwide Class's PII and PHI was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

119. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

120. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

121. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

122. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

123. The harm that occurred as a result of the Cybersecurity Event is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

124. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use

of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Cybersecurity Event, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the current and former patients' PII and PHI in their continued possession; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Cybersecurity Event for the remainder of the lives of Plaintiff and the Nationwide Class.

125. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

126. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI in their continued possession.

127. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff are at an increased risk of identity theft or fraud.

128. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff are entitled to and demand actual consequential, and nominal damages and injunctive relief.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and the Nationwide Class)

129. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

130. Defendants acquired and maintained the PII and PHI of Plaintiff and the Nationwide Class, including names, addresses, dates of birth, and/or Social Security numbers as well as health insurance information, medical record numbers, patient account numbers, and/or limited treatment information.

131. Prior to the Cybersecurity Event, Defendants published the Privacy Notice, agreeing to protect and keep private medical information of Plaintiff and the Nationwide Class.

132. In collecting and maintaining the PII and PHI of Plaintiff and the Nationwide Class and publishing the Privacy Notice, Defendants entered into contracts with Plaintiff and the Nationwide Class requiring Defendants to protect and keep private medical information of Plaintiff and the Nationwide Class.

133. Plaintiff and the Nationwide Class fully performed their obligations under the contracts with UFHCF.

134. Defendants breached the contracts they made with Plaintiff and the Nationwide Class by failing to protect and keep private medical information of Plaintiff and the Nationwide Class, including failing to (i) encrypt or tokenize the sensitive PII and PHI of Plaintiff and the Nationwide Class, (ii) delete such PII and PHI that it no longer had reason to maintain, (iii)

eliminate the potential accessibility of the PII and PHI from the Internet, and (iv) otherwise review and improve the security of its computer system that contained such PII and PHI.

135. As a direct and proximate result of Defendants' above-described breach of contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

136. As a direct and proximate result of Defendants' breach of contract, Plaintiff are at an increased risk of identity theft or fraud.

137. As a direct and proximate result of Defendants' breach of contract, Plaintiff are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

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

138. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

139. A relationship existed between Plaintiff and the Nationwide Class and Defendants in which Plaintiff and the Nationwide Class put their trust in Defendants to protect the private information of Plaintiff and the Nationwide Class and Defendants accepted that trust.

140. Defendants breached the fiduciary duty that they owed to Plaintiff and the Nationwide Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the Nationwide Class.

141. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and the Nationwide Class.

142. But for Defendants' breach of fiduciary duty, the damage to Plaintiff and the Nationwide Class would not have occurred.

143. Defendants' breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Nationwide Class.

144. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and

Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' personal identifying information;

v. prohibiting Defendants from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as

necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

Date: September 3, 2021 Respectfully Submitted,

/s/ John A. Yanchunis
JOHN A. YANCHUNIS
RYAN D. MAXEY
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Exhibit 1

Privacy policy

Effective date: April 14, 2003
Revised date: February 17, 2010
Revised date: September 23, 2013

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY.

If you have any questions about this notice, please contact the privacy officer at 352.323.5924, or write to the UF Health Central Florida Privacy Officer, Compliance and Legal Department, 600 East Dixie Avenue, Leesburg Florida, 34748.

Who will follow this notice

This notice describes UF Health Central Florida's practices and that of (a) any healthcare professional authorized to enter information into your medical record, (b) all departments and units of the system, (c) volunteers we allow help you while you are in the facility, and (d) all members of the healthcare system's workforce.

All of the UF Health Central Florida's entities, sites and locations follow the terms of this notice, including but not limited to: UF Health Leesburg Hospital, UF Health The Villages® Hospital, UF Health The Villages® Hospital Rehabilitation Hospital, UF Health Leesburg Hospital Urgent Care Center, UF Health Alliance Laboratory, and all other affiliated sites and locations.

Contracted services also follow the terms of this notice, including any contracted physician/clinician services and all other individuals providing services at UF Health Central Florida. These individuals, entities and facilities may share medical information with each other for payment, treatment or hospital operations purposes as described in this notice.

Our pledge regarding medical information

We understand that medical information about you and your health is personal. We are committed to protecting that medical information. We create a record of the care and services you receive to provide you with quality care and to comply with certain legal requirements.

This notice applies to all of the records of your care generated by UF Health Central Florida, whether made by organization personnel or your personal physician. Your personal physician may have different policies or notices regarding his/her use and disclosure of medical information created in his/her office or clinic. This notice tells you about the ways in which we may use and disclose information about you. It also describes your rights and certain obligations we have regarding the use and disclosure of medical information.

Notice of privacy practices

We are required by law to make sure that health-related information that identifies you is kept private; give you this notice of our legal duties and privacy practices with respect to medical information about you; and follow the terms of the notice that is currently in effect.

How we may use and disclose medical information about you

The following categories describe the ways that we may use and disclose health-related information. For each category of uses or disclosures we will explain what we mean and try and give examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of these categories.

For treatment. We may use and disclose information about you to provide you with medical treatment or services. We may disclose medical information about you to physicians, nurses, technicians, medical students or other hospital personnel who are involved in your care. (For example, a physician treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. In addition, the physician may need to tell the dietician if you have diabetes so we can arrange appropriate meals.)

Departments of the hospital also may share medical information about you in order to coordinate the things you need, such as prescriptions, lab work, and x-rays. We also may disclose medical information about you to people outside the hospital who may be involved in your medical care after you leave the hospital, such as family members, clergy or others who provide services that are part of your care.

For payment. We may use and disclose medical information about you so the treatment and services you receive at the hospital may be billed to and payment may be collected from you, an insurance company or a third party. (For example, we may need to give your health plan information about surgery you received so your health plan will pay us or reimburse you for the surgery). We may also tell your health plan about treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment.

For healthcare operations. We may use and disclose information about you for normal hospital operations. These uses and disclosures are necessary to run the facility and make sure all our patients receive quality care. (For example, in the course of quality assurance activities, we may use medical information to review our treatment and services and to evaluate the performance of our staff in caring for you.) Some of these reviews may be conducted by independent physicians who are members of the medical staff but not employees. We may disclose medical information to business associates who provide contracted services such as accounting, legal representation, claims processing, accreditation and consulting. If we do disclose medical information to a business associate, we will do so subject to a contract that provides the information will be kept confidential. We may also combine medical information about many hospital patients to decide what additional services the hospital should offer, what services are not needed and whether certain new treatments are effective. We may also disclose information to physicians, nurses, technicians, medical students and other personnel for review and learning purposes. We may also combine the medical information we have with medical information from other facilities to compare how we are doing and see where we can make improvements in the care and services we offer. We may remove information that identifies you from this set of medical information so others may use it to study healthcare and healthcare delivery without learning who the specific patients are.

Appointment reminders. We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment.

Follow-up phone calls. As part of your treatment plan, there may be times that you will be contacted by the healthcare system's staff via telephone after you have a service. Examples include (1) follow-up phone call after discharge from the hospital to answer any questions from the patient or family or to determine that the patient is recovering appropriately, (2) phone call to address patient satisfaction issues or (3) phone call to provide additional education or guidance to the patient on a particular topic related to his or her hospital stay or (4) phone call to assist with claim processing and payment. Such phone calls will be limited and are meant to ensure optimum recovery, patient satisfaction and education.

Treatment alternatives and health-related benefits and services. We may use and disclose medical information to recommend or tell you about treatment alternatives and health-related benefits or services that may be of interest to you. UF Health Central Florida promotes community awareness of services provided by the organization. Materials sent only reflect the services available and the level of licensure and accreditation. Any unsolicited materials you receive from the healthcare system will have information on how the recipient can opt out of future mailings. To exercise your option not to receive unsolicited information from the healthcare system, please notify us by e-mail at the following address; info@centflhealth.org or calling **352.323.7777**.

Fundraising activities. We may use medical information about you to contact you in an effort to raise money for the healthcare system and its operations. We can release the following information; demographic information such as your name, address, contact information, age, gender, date of birth, health insurance status, treating physician, department of service, and outcome information. If

you do not want the hospital to contact you for fundraising efforts, you can notify us by returning the self-addressed envelope indicating you have opted out from future mailings, send an e-mail to info@centflhealth.org or call **352.323.7777**.

Hospital directory. We may include certain limited information about you in a hospital directory listing while you are an inpatient or observation patient in one of our hospitals. This information may include your name, location in the hospital, your general condition (fair, stable, etc.) and your religious affiliation. The directory information, except for your religious affiliation, may be released to people who ask for you by name. Your religious affiliation may be given to a member of our clergy, such as a priest or rabbi, even if they do not ask for you by name. This is so your family, friends and clergy can visit you in the hospital and generally know how you are doing.

Individuals involved in your care or payment for your care. We may release medical information about you to a friend or family member who is involved in your medical care. We may also give information to someone who helps pay for your care. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.

Research. Under certain circumstances, we may use and disclose medical information about you for research purposes. (For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another for the same condition.) All research projects are subject to a special approval process. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with patients need for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process, however, we may disclose medical information about you to people preparing to conduct a research project to help them look for patients with specific medical needs, as long as the medical information they review does not leave the healthcare system. When our staff conducts a research project, in which they look at old medical records, your personal information will not be disclosed outside the hospital nor will you be identified in any reports. If a research project is conducted where your information cannot be held confidential, a separate process is in place for you to consent for this type of research.

Service excellence. We may follow up your visit with us by sending to the address listed in your records a brief written survey about your satisfaction with the level of service provided to you. In some cases, the survey may be conducted by telephone or e-mail using the contact information listed in your medical record. In some instances your name may be passed on to members of the Service Excellence Team to investigate a complaint or corroborate an incident.

As required by law. We will disclosure medical information about you when required to do so by federal, state or local law.

To avert a serious threat to health or safety. We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety of the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

Special situations

Organ and tissue donation. We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety of the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

Military and veterans. If you are a member of the armed forces, we may release medical information about you as required by military authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authorities.

Workers' compensation. We may release medical information about you for workers compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public health risks. We may disclose medical information about you for public health activities. These activities generally include the following: (a) to prevent or control disease, injury or disability; (b) to report births and deaths; (c) to report child abuse or neglect; (d) to report reactions to medications or problems with products; (e) to notify people of recalls of products they may be using; (f) to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; (g) to notify the appropriate government authority if we believe you have been the victim of abuse, neglect or domestic violence.

Health oversight activities. We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections and licensure. These activities are necessary for the government to monitor the healthcare system, government programs and compliance with applicable laws.

Lawsuits and disputes. If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to

obtain an order protecting the information requested.

Law enforcement. We may release medical information if asked to do so by a law enforcement official: (a) in response to a court order, subpoena, warrant, summons or similar process; (b) to identify or locate a suspect, fugitive, material witness, or missing person; (c) about a victim of a crime if, under certain circumstances, we are unable to obtain the persons agreement; (d) about a death we believe may be the result of criminal conduct; (e) about criminal conduct at the hospital; (f) in emergency circumstances to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

Coroners, medical examiners and funeral directors. We may release medical information to identify a deceased person or determine the cause of death. We may also release medical information about patients of the hospital to funeral directors as necessary to carry out their duties.

National security and intelligence activities. We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

Protective services for the president of the United States. We may disclose medical information about you to authorized federal officials so they may conduct special investigations and provide protection to the President or other officials and dignitaries.

Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary for the institution to provide you with healthcare, to protect yours and others health and safety, or for the safety and security of the correctional institution.

Your rights regarding medical information about you

You have the following rights regarding the medical information we maintain about you.

Right to inspect and copy. You have the right to inspect and copy medical information that may be used to make decisions about your care, this usually includes medical and billing records. To inspect and copy medical information that may be used to make decisions about you, you must submit your request in writing to Health Information Services, UF Health Leesburg Hospital, 600 East Dixie Avenue, Leesburg, FL 34748 or Health Information Services, UF Health The Villages® Hospital, 1451 El Camino Real, The Villages, FL 32159. If you request a copy of the information we may charge a fee for the costs of copying, mailing or other supplies associated with your request. If you have questions about this prior to asking for this information in writing, please call either the Leesburg health information services department at **352.323.5420** or The Villages health information services department at **352.751.8846**. We may deny your request to inspect and copy your medical information in certain limited circumstances. If you are denied access to medical information you may request the denial be reviewed. Another licensed healthcare professional chosen by the hospital will review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

Right to an electronic copy of electronic medical records. You have the right to access and request an electronic copy of your record be given to you or sent to another individual or entity.

Right to amend. If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for UF Health Central Florida.

Requests to amend a medical record must be made in writing and submitted to the health information services department, UF Health Leesburg Hospital, 600 East Dixie Avenue, Leesburg, FL 34748 or to the health information services department, UF Health The Villages® Hospital, 1451 El Camino Real, The Villages, FL 32159. If you do so in person, there is a form that will be provided to you to request this amendment. In addition, you must provide a reason that supports your request.

To request an amendment while you are a patient in the facility, you may ask the caregiver who made the chart entry (physician, nurse, therapist). This person will include your request as a progress note in the chart to show the clarification, correction or response.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that (a) was not created by us, unless the person or entity that created the information is no longer available to make the amendment; (b) is not part of the medical information kept by or for the hospital; (c) is not part of the information which you would be permitted to inspect and copy; or (d) is accurate and complete.

Right to receive notice of any breach unsecured PHI. We are required to notify patients of any breach of unsecured PHI. Generally a breach is a defined as unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information. Security and privacy are considered compromised when the disclosure poses a high probability of financial, reputational or other risk to the member.

The notice of breach must be sent to the patient no later than 60 days from the date the breach was discovered. It must contain a description of the breach and type(s) of unsecured PHI involved in the breach, protective measures the patient should take, if any, to protect against losses and actions taken by UF Health Central Florida to investigate and mitigate any losses from the breach.

Right to an accounting of disclosures. You have the right to request an accounting (list) of certain types of disclosures we have made of medical information about you. We are not required to account for disclosures that were (a) authorized by you; (b) to carry out treatment, payment and health care operations; (c) to you of health information about you; (d) for our facility directory; (e) for purposes of notifying persons involved in your care of your location, general condition or death; (f) for national security or intelligence purposes; or (g) to correctional institutions or law enforcement officials as noted above. To request an accounting of disclosures, you must submit your request in writing to the health information services department, UF Health Leesburg Hospital, 600 East Dixie Avenue, Leesburg, FL 34748 or to the health information services department, UF Health The Villages® Hospital, 1451 El Camino Real, The Villages, FL 32159.

Your request must state a time period, which may not be longer than six years and may not include dates before April 14, 2003. Your request should indicate in what form you want the list (for example, on paper or electronically). The first list you request within a 12 month period will be free. For additional lists we may charge you for the costs of providing the list. We will notify you of the costs involved and you may choose to withdraw or modify your request at that time before costs are incurred. If you have questions about this prior to asking for this information in writing, please call the Leesburg health information services department at **352.323.5240** or The Villages health information services department at **352.751.8846**.

Patients have the right to receive an accounting of electronic health records disclosures of PHI (including disclosures for purposes of payment, treatment or healthcare operations), but only for a 6 year period prior to the date of the request. We may charge you for the costs of providing the list.

Right to request restrictions. You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment of healthcare operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. (For example, you could ask that we not use or disclose information about a surgery you had or you could ask that information about you not be included in the facility directory).

If you have paid out-of-pocket (or in other words, you have requested that we not bill your health plan) in full for a specific item or service, you have the right to ask that your PHI related to that item or service not be disclosed to your health plan for the purposes of payment, treatment or health care operations and we will honor this request.

If you want to request a restriction, you must complete a Request to Invoke/Revoke Restrictions on Disclosure of Protected Health Information available at any admission or registration area or submit your request in writing to UF Health Leesburg Hospital, health information services department, 600 East Dixie Avenue, Leesburg, FL 34748 or UF Health The Villages® Hospital, health information services department, 1451 El Camino Real, The Villages, FL 32159. The written request must include (1) what information you want to limit); (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply (for example, disclosure to your spouse or other family members). We will reply to you within 60 days.

Right to request confidential communications. You have the right to request we communicate with you about medical matters in a certain way or at a certain location. (For example, you can ask that we only contact you at work or by mail). To request confidential communications, you must make your request in writing to the health information services department, UF Health Leesburg Hospital, 600 East Dixie Avenue, Leesburg, FL 34748 or the health information services department, UF Health The Villages® Hospital, 1451 El Camino Real, The Villages, FL 32159. We will not ask you the reason for the request, and will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

Written authorization required for other uses and disclosures. The following uses and disclosures of your PHI will be made only with your written authorization (a) most uses and disclosures of psychotherapy notes; (b) uses and disclosures of PHI for marketing purposes; (c) disclosures that constitute the sale of your PHI; (d) other uses and disclosures not covered by this notice.

If you give us an authorization to use or disclose medical information about you, you may revoke that authorization at any time by submitting in writing your revocation including the date and specific authorization involved. Submit this request to Health Information Services, UF Health Leesburg Hospital, 600 East Dixie Avenue, Leesburg, FL 34748 or Health Information Services, UF Health The Villages® Hospital, The Villages, FL 32159.

Uses and disclosures made on your authorization before you revoked it will not be affected by the revocation. You understand that we are unable to take back any disclosures we have already made with your permission, and we are required to retain our records of the care we provided to you.

Right to a paper copy of this notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you agree to receive this notice electronically, you are still entitled to a paper copy of this notice. To obtain a paper copy of this notice, go to any UF Health Leesburg Hospital or UF Health The Villages® Hospital information desk, admitting/registration area or health information services department.

Changes to this notice

We reserve the right to change this notice at any time. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current notice in the hospital. The notice will contain on the first page the effective date. Revised copies of this notice will be available at your next visit.

Complaints

If you believe your privacy rights have been violated, you may file a complaint with the facility or with the Secretary of the U.S. Department of Health and Human Services. To file a complaint with the facility, contact the privacy officer, Compliance and Legal Department, UF Health Central Florida, 600 East Dixie Avenue, Leesburg, FL 34748. All complaints must be submitted in writing and you will not be penalized or retaliated against for filing a complaint.

Organized healthcare arrangement

UF Health Central Florida, the independent contractor members of its medical staff (including your physician) and other healthcare providers affiliated with UF Health Central Florida have agreed, as permitted by law, to share your health information among themselves for purposes of your treatment, payment or healthcare operations. This enables us to better address your healthcare needs.

Download a copy of our privacy policy.

Contact us
UF Health Leesburg Hosp
600 E. Dixie Ave.
Leesburg, FL 34748
352.323.5762

Education and resources

Calendar
Community benefit report
Community Medical Care Center
Email Newsletters
Health library
Healthy You, Healthy Us
Organ Donation

Employment

Current employees
External applicants
Physician opportunities

Foundation/volunteering

Foundation
- Giving opportunities
- Center for Excellence in Nursing
- Royal Palm Society
- Donate online
- Our team
- Events

Volunteering

Privacy policy |

Exhibit 2

Notice to Our Patients of Cybersecurity Event

UF Health takes the privacy and security of our patients' information very seriously. This notice concerns a cybersecurity event that may have involved some of that information.

On May 31, 2021, UF Health Central Florida — including UF Health Leesburg Hospital and UF Health The Villages® Hospital — detected unusual activity involving its computer systems. We took immediate action to contain the event, including reporting it to law enforcement and launching an investigation with independent experts. UF Health's Gainesville or Jacksonville campuses were not affected.

The investigation determined that unauthorized access to UF Health Central Florida's computer network occurred between May 29 and May 31, 2021. During this brief time period, some patient information may have been accessible, such as names, addresses, dates of birth, Social Security numbers, health insurance information, medical record numbers and patient account numbers, as well as limited treatment information used by UF Health for its business operations. UF Health's electronic medical records were not involved or accessed.

We have no reason to believe the information was further used or disclosed; however, on July 30, 2021, we began mailing letters to individuals whose data may have been involved and, as a precautionary measure, are offering them complimentary credit monitoring and identity protection services. Patients are also encouraged to review statements from their health insurer, and to contact them immediately if they see any services they did not receive. We also established a dedicated call center for patients to call with questions. If you believe you are affected, but do not receive a letter by Aug. 16, 2021, please call 1-833-909-3926 between 9 a.m. and 9 p.m. Eastern Time Monday through Friday.

UF Health takes this issue very seriously and is committed to taking steps to help prevent something like this from happening again, including enhancing the security of our electronic systems and the information we maintain.

Awards and recognitions
Advisory board
Care Delivery Alliance
- Care Delivery Alliance physicians
- Resources

Community Health Needs Assessment
Executive team
Fast Facts
Message from Heather Long
Mission and vision
News center
UF Health The Villages® Hospital

Patients and visitors

Advance directives
Electronic health record
Health plans accepted
Healthcare price transparency
- Accepted health plans

Commitment to the Community
Online bill pay
Patient information
Patient rights and responsibilities
- Nondiscrimination and accessibility notice

Physician directory
Registration
- Online appointments

Reminders During COVID-19
Translation Services
Website Accessibility Statement

Services

Behavioral health
Cancer care
Cardiac Care
- Heart Attack Signs and Symptoms
- Cardiac rehabilitation
- Conditions treated
- Heart valve surgery
- Interventional cardiology
- Cardiovascular surgery

Chest Pain Center
Emergency services
Imaging services
- Women's Imaging

Laboratory
Neurosciences
Orthopedics
Palliative Care
- Staff Resources
- Patient and Family Resources

Pediatrics
Pre-procedure Assessment Center
Rehabilitation services
Stroke Center
Surgical services
Urgent care
- When to go to the emergency room

Weight Loss
Women's health
Wound care

Education and resources

Calendar
Community benefit report
Community Medical Care Center
Email Newsletters
Health library
Healthy You, Healthy Us
Organ Donation

Employment

Current employees
External applicants
Physician opportunities

Foundation/volunteering

Foundation
- Giving opportunities
- Center for Excellence in Nursing
- Royal Palm Society
- Donate online
- Our team
- Events

Volunteering

UF Health Leesburg Hosp
600 E. Dixie Ave.
Leesburg, FL 34748
352.323.5762

Privacy policy |

ClassAction.org