CASE NO. 23-CI-003349
Electronically filed

JEFFERSON CIRCUIT COURT
DIVISION TWO (2)
JUDGE ANNIE O'CONNELL

ABBY BERTHOLD, CHARLOTTE D'SPAIN, and LANISHA MALONE, individually, on behalf of themselves, and all others similarly situated **PLAINTIFFS**

v. **SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**

NORTON HEALTHCARE, INC.
-and-
NORTON HOSPITALS, INC. **DEFENDANTS**

* * * * * * * * * * * *

Come now the Plaintiffs, ABBY BERTHOLD (hereinafter "Plaintiff Berthold") CHARLOTTE D'SPAIN ("Plaintiff D'Spain") and LANISHA MALONE ("Plaintiff Malone") (collectively, "Plaintiffs") individually, on behalf of themselves, and all others similarly situated, and for their causes of action against the Defendants, NORTON HEALTHCARE, INC. and NORTON HOSPITALS, INC. (collectively, "Norton" or "Defendants"), their Second Amended Consolidated Class Action Complaint, allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. On or about May 9, 2023, Defendants lost control of the confidential Personally Identifying Information ("PII")[1] and Protected Health Information ("PHI")[2] (collectively, "PHI")

[1] The Federal Trade Commission defines "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." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of

of Plaintiffs and the Class Members, current and former patients and employees of Norton, in a ransomware cyberattack on their systems, caused by Defendants' failure to adequately safeguard that PHI ("the Data Breach").

2. Norton is a massive, not-for-profit health care system headquartered in Louisville, Kentucky, "a leader in serving adult and pediatric patients from throughout Greater Louisville, Southern Indiana, the commonwealth of Kentucky and beyond."[3]

3. Norton failed to undertake adequate measures to safeguard the PHI of Plaintiffs and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

4. Although Norton discovered the Data Breach on or about May 9, 2023, Defendants have failed, and continue to fail, to notify and warn affected persons, Norton's current and former patients and employees, of the Data Breach and compromise of their PHI therein.

5. As a direct and proximate result of Defendants' failures to protect current and former patients and employees' sensitive PHI and warn them promptly and fully about the Data Breach, Plaintiffs and the proposed Class Members have suffered widespread injury and damages necessitating Plaintiffs seeking relief on a class wide basis.

---

healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). Both Norton Healthcare, Inc. and Norton Hospitals, Inc. are clearly each a "covered entity" and some of the data compromised in the Data Breach that this action arises out of is "protected health information," subject to HIPAA.

[3] Norton Healthcare, Inc. and Norton Hospitals, Inc. website, available at https://nortonhealthcare.com/about-us/ (last accessed July 7, 2023)

PARTIES

6. Plaintiff Berthold is a citizen of the Commonwealth of Kentucky, with a residence in Louisville Metro., Jefferson County, Kentucky, where she intends to remain.

7. Plaintiff D'Spain is a citizen of the Commonwealth of Kentucky, with a principal residence in Louisville Metro., Jefferson County, Kentucky, where she intends to remain.

8. Plaintiff Malone is a citizen of the State of Indiana, with a principal residence in New Albany, Floyds County, Indiana, where she intends to remain.

9. Defendant Norton Healthcare, Inc., is a non-profit corporation organized and existing under the laws of the Commonwealth of Kentucky with its principal place of business located in Louisville Metro., Jefferson County, Kentucky at 4967 US Highway 42, Suite 101, Louisville, Kentucky 40222-6363.

10. Defendant Norton Hospitals, Inc., is a non-profit corporation organized and existing under the laws of the Commonwealth of Kentucky with its principal place of business located in Louisville Metro., Jefferson County, Kentucky at 4967 US Highway 42, Suite 101, Louisville, Kentucky 40222-6363.

11. On information and belief, Defendants Norton Healthcare, Inc. and Norton Hospitals, Inc. are *alter egos* of one another, and are collectively referred to as "Defendants" or "Norton" herein.

JURISDICTION AND VENUE

12. This Court has personal jurisdiction over Defendants as they each maintain a principal place of business in the Commonwealth and conduct business here, such that they are at home within Kentucky.

13. The Court has subject matter jurisdiction pursuant to KRS § 23A.010.

14. Venue is proper in Jefferson County under KRS § 452.460, because Defendants each maintain a principal place of business in this County.

FACTUAL BACKGROUND

A. Defendants, Norton Healthcare, Inc., and Norton Hospitals, Inc.

15. Norton is a massive healthcare system based in Louisville Metro., Jefferson County, Kentucky which owns and operates numerous hospitals, outpatient medical centers, and physicians' practices, which renders medical treatment to approximately 600,000 patients a year.[4]

16. As Norton describes:

> The system includes six hospitals (five in Louisville and one in Madison, Indiana) with 1,993 licensed beds, eight outpatient centers, 18 Norton Immediate Care Centers, eight Norton Prompt Care at Walgreens clinics and an expanded telehealth program. It provides care at more than 340 locations throughout Kentucky and Southern Indiana. The hospitals provide inpatient and outpatient general care as well as specialty care including heart, neuroscience, cancer, orthopedic, women's and pediatric services. A strong research program provides access to clinical trials in a multitude of areas.[5]

17. Defendants own and operate Norton Audubon Hospital, Norton Brownsboro Hospital, Norton Children's Hospital, Norton Children's Medical Center, and Norton Hospital in Louisville, Kentucky; Norton King's Daughters' Hospital in Madison, Indiana; and Norton Women's and Children's Hospital in Louisville, as well as diagnostic centers, immediate care centers, prompt care centers at Walgreens, pediatric after hour care centers, outpatient treatment centers, as well as pharmacies, primary care physicians, and specialist care.[6]

18. As described by Norton Healthcare, Inc. "[i]n 2021 Norton Healthcare**, through its**

---

[4] *See* WDRB, "Norton Healthcare offers guidance on accessing care, answering questions following cyberattack," May 25, 2023, available at https://www.wdrb.com/news/business/norton-healthcare-offers-guidance-on-accessing-care-answering-questions-following-cyberattack/article_eca728d2-fb26-11ed-a586-dfb337b4ba4b.html (last accessed July 7, 2023).
[5] Norton website, available at https://nortonhealthcare.com/about-us/ (last acc. July 7, 2023).
[6] *See* https://nortonhealthcare.com/location/?facilities=norton&type=570 (last acc. July 7, 2023).

affiliate, Norton Hospitals Inc., had a total of 1,907 licensed beds: Norton Audubon Hospital, 432 beds; Norton Brownsboro Hospital, 197 beds; Norton Children's Hospital, 300 beds; Norton Hospital, 605 beds; and Norton Women's & Children's Hospital, 373 beds. these five hospitals operate 24 hours a day, seven days a week," as well as operating through other affiliates such as Community Medical Associates, Inc.[7]

19. Indeed, Norton Hospitals, Inc. provides medical services at many facilities, under assumed names of: Norton Hospital; Norton Brownsboro Hospital; Norton Children's Hospital; Norton Children's Hospital Outpatient Center; Norton Women's and Children's Hospital; Norton Neurosciences & Spine Rehabilitation Center; Norton Healthcare Pavilion; Norton Audubon Hospital; Women's Pavilion Breast Center; Norton Infectious Diseases Specialists; Norton Breast Health Program; Eating Disorders Coalition of Kentuckiana; Norton Cancer Institute Research Program; Norton Rheumatology; Kentucky Podiatric Residency Program; Addison Jo Blair Cancer Care Center; Woody And Lucille Stephens Cardiac and Pulmonary Rehabilitation Center; Norton Wound Healing Center; Norton Diagnostic Center - Fern Creek; Kentucky Regional Poison Control Center; Norton Multispecialty Clinic; Norton Healthcare International Patient Care; Norton Medical Plaza at Old Brownsboro Crossing; Norton Pediatric Ambulatory Surgery Center; Norton Home Health; Norton Diagnostic Center – Dixie; Center for Advanced Orthopaedics of Norton Hospital; Kenton D. Leatherman Spine Center; Norton Children's Prevention and Wellness; Norton Cancer Institute Radiation Center; Norton Health and Wellness Center; Norton Sports Health; Norton Women's' Heart Center; Baby Bistro & Boutique; Norton Diagnostic Center – Brownsboro; Norton Children's Cancer Institute; Norton Cancer Institute; Norton Cardiovascular

[7] Norton Healthcare, Inc. Form 990, Return of Organization Exempt From Income Tax, 2021 ("Norton Healthcare, Inc. Form 990") avail. at https://nortonhealthcare.com/wp-content/uploads/2022/12/2021-NHC-990-PublicDisclosure.pdf, pp. 2, 67 (emphasis added) (last accessed Oct. 26, 2023).

Diagnostic Center; Cressman Neurological Rehabilitation; Norton Specialty Rehabilitation Center; Norton Healthcare Center for Prevention and Wellness; Norton St. Matthews Infusion Center; Norton Weight Management Services; Norton Women's Pavilion; Pediatric After Hours Program; Healthy For Life Alliance; Norton Diagnostic Center – Dupont; Norton Healthcare Hereditary Cancer Institute; Norton Healthcare Louisville Hospital System; Norton Sports Health Performance and Wellness Center; Norton Children's International Patient Care; Norton Children's Medical Center; Norton Children's Medical Center - Pediatric Outpatient Center; Norton Children's After Hours; Norton Children's Heart Center; Norton Audubon Hospital Heart & Vascular Institute; Norton Healthcare Transport; Norton West Louisville Hospital (upcoming]; Grief Care; Family Link; and, Just For Kids Transport.[8]

20. Norton Healthcare, Inc. is the controlling and supporting organization of Norton Hospitals, Inc., performing Defendants' management and administrative functions, allowing them to provide medical services as a collective healthcare system:

> The management of Norton Healthcare, Inc. is vested in the same persons that control and manage the supported organizations. Specifically, the organizations share the same president/chief executive officer, chief legal officer, executive vice president/chief operating officer, and chief financial officer. **This common control allows Norton Healthcare, Inc. and its four supported organizations to function collectively as a health system, with Norton Healthcare, Inc. providing management and administrative support to the supported organizations.** The fact that the core leadership team of each of the supported organizations is also the core leadership team of Norton Healthcare, Inc. assures that Norton Healthcare, Inc. is responsive to the needs and demands of the supported organizations and that Norton Healthcare, Inc. constitutes an integral part of and maintains a significant involvement in the operations of the supported organizations.[9]

21. In this collective healthcare system, Norton provides medical services to patients

[8] *See* Kentucky Secretary of State, Business Entity Search, "Norton Hospitals, Inc." assumed names, avail. at https://web.sos.ky.gov/bussearchnprofile/Profile/?ctr=369947 (last acc. Oct. 26, 2023).
[9] Norton Healthcare, Inc. Form 990, pg. 22.

including emergency department treatment, general surgery, behavioral health, brain tumor, breast health, cancer care, diabetes & endocrinology, gastroenterology, geriatric care, heart & vascular, hematology, home health, imaging diagnostics, immediate care, infectious diseases, kidney, bladder & urinary, liver & pancreas, lymphedema, neuroscience, occupational medicine, orthopedics, pain management, palliative care, prevention & wellness, primary care, prompt care clinics, pulmonary, rehabilitation, research & clinical trials, rheumatology, sleep center, spine care, sports health, telehealth, weight management, women's health, and wound care.[10]

22. In addition, Norton is Louisville, Kentucky's "second largest employer, with more than 18,000 employees, over 1,700 employed medical providers and approximately 2,000 total physicians on its medical staff."[11]

23. Norton Healthcare, Inc. is the "common paying agent" for Norton Hospitals, Inc. and the other supported organizations.[12]

24. Norton Healthcare, Inc. and Norton Hospitals, Inc. operate and utilize the same website, https://nortonhealthcare.com/.[13]

25. Upon information and belief, as a condition of rendering medical treatment to patients, and as a condition of employment with Defendants, Norton requires that their patients and employees disclose their PHI, including: (1) for patients, their full names, dates of birth, addresses, telephone numbers, Social Security numbers, medical information such as diagnostic data, treatment data, insurance data, prescription data, imaging data, lab data, as well as financial

[10] https://nortonhealthcare.com/location/?facilities=norton&type=570 (last acc. Oct. 26, 2023).
[11] https://nortonhealthcare.com/about-us/
[12] Norton Healthcare Form 990, pg. 74.
[13] See Norton Healthcare Form 990, pg. 1; and Norton Hospitals, Inc. Form 990, Return of Organization Exempt From Income Tax, 2021 ("Norton Hospitals, Inc. Form 990") avail. at https://nortonhealthcare.com/wp-content/uploads/2022/12/2021-NH-990-PublicDisclosure.pdf , pg. 1, both referring to website nortonhealthcare.com.

information; (2) for employees their names, addresses, phone numbers, Social Security numbers, banking routing and account numbers, driver's license, date of birth; and (3) for patients and employees, their Credit card numbers with names, addresses, and CVV codes.

26. In exchange for this information, Norton promises to safeguard their patients' and employees' PHI, and to only use this confidential information for authorized purposes.

27. Defendants acknowledge the importance of properly safeguarding the private data and PHI of their patients and employees, maintaining a Notice of Privacy Practices which states, "[w]e understand that medical information about the health of our patients is personal. We are committed to protecting patients' personal medical information."[14]

28. Norton's Notice of Privacy Practices applies to Norton Healthcare's practices, and:

- Any health care professional authorized to enter information into a patient's chart
- All departments and units within Norton Healthcare facilities
- Any member of a volunteer group that Norton Healthcare allows to help patients while they are in a Norton Healthcare facility
- All employees, staff and other Norton Healthcare facility personnel and participating members of the medical staffs
- Norton Healthcare hospitals, physician practices and any other owned or managed entities of Norton Healthcare[15]

29. In the Notice of Privacy Practices, Norton states, represents, and promises:

Norton Healthcare is required by law to:

- Make sure medical information that identifies patients is kept private
- Give patients this notice of our legal duties and privacy practices with respect to patients' medical information
- Obtain an acknowledgment from each patient regarding receipt of this notice
- Follow the terms of the notice that are currently in effect
- Notify affected individuals following a breach of unsecured protected

[14] Norton Notice of Privacy Practices, available at https://nortonhealthcare.com/hipaa/ (last acc. July 7, 2023), **attached as Exhibit A.**
[15] *Id*.

health information[16]

30. In addition, Defendants' Notice of Privacy Practices provide certain purposes for which PHI may be disclosed, including, *inter alia*, for treatment; for payment; for health care operations; for appointment reminders; for treatment alternatives; for health-related benefits and services; for fundraising activities; for certain marketing activities; for a hospital directory; to individuals involved in care or payment of care; for research; to avoid a serious threat to health or safety; to business associates; for health information exchanges; and for other purposes.[17]

31. None of these permitted purposes for Norton's disclosure of PHI as set forth in the Notice of Privacy Practices include the Data Breach.

32. In addition, Norton, by and through their agents and employees, represented to their current and former employees and patients, that Defendants would adequately protect their PHI and not disclose said information other than as authorized, including as set forth in their Notice of Privacy Practices.

33. Plaintiffs and the proposed Class Members, including current and former patients and employees of Norton, entrusted their PHI to Defendants, and would not have done so in the absence of Defendants' promises to safeguard that information, including in the manner set forth in Defendants' Notice of Privacy Practices.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the proposed Class Members' PHI, Defendants assumed legal and equitable duties to Plaintiffs, and the members of the Proposed Class, and knew or should have known that it was responsible for protecting their PHI from unauthorized disclosure.

35. At all times Plaintiffs and the members of the Proposed Class have taken reasonable

---

[16] *Id*.
[17] *Id*.

steps to maintain the confidentiality of their PHI; and, Plaintiffs and the proposed Class Members, as current and former patients and employees of Norton, relied on Defendants to keep their PHI confidential and securely maintained.

B. Norton Fails to Adequately Safeguard Current and Former Patients' and Employees' PHI—the Data Breach

36. Plaintiffs and the proposed Class Members are current and former patients and employees of Defendants, Norton Healthcare, Inc. and/or Norton Hospitals, Inc. ("Norton").

37. As a condition of receiving Norton's medical services and/or as a material condition of employment, Defendants required Plaintiffs and the proposed Class Members to provide Norton with their sensitive, PHI, including names, dates of birth, Social Security Numbers, and financial information, specifically for both patients and employees:

- Names, addresses, telephone numbers, and email addresses;
- Dates of birth;
- Social Security numbers;
- Marital status;
- Employers with contact information;
- Primary and secondary insurance policy holders' name, address, date of birth;
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage;
- Banking and/or credit card information; and,
- Other information

(collectively, "PHI").

38. Norton then collected and maintained this PHI in their computer information technology systems and networks, including on information and belief, those servers located at their headquarters in Jefferson County, Kentucky.

39. On information and belief, beginning on or about May 9, 2023, the PHI of Norton's current and former patients and employees—Plaintiffs and the Class Members—was unauthorizedly disclosed to third-party cybercriminals and compromised during the Data Breach cyberattack to Defendants' computer network systems, and then posted to the Dark Web.

40. On May 11, 2023, Defendants posted a vague notification on their website, https://nortonhealthcare.com/, the "Norton Healthcare Network Update" ("May 11, 2023 Network Update") stating that on the prior Tuesday, May 9, 2023, Norton was the victim of a cyber-event, "when the security team received a suspicious communication related to information systems."[18]

41. The May 11, 2023 Network Update further stated that following Norton's discovery of the cyber-event, Defendants worked with their information technology team and cybersecurity experts to "determine the scope of the event," "notified law enforcement," and took their systems offline and disabled email access to protect their networks.[19]

42. In the May 11, 2023 Network Update, Norton also represented that "[h]ospitals, other facilities and medical practices remain[ed] open while caregivers follow protocols for times in which systems are down. Patients should continue to arrive for appointments at regular times unless otherwise contacted by phone."[20]

43. The May 11, 2023 Network Update provided little other information, and failed to

[18] "Norton Healthcare Network Update," May 11, 2023, originally available at https://nortonhealthcare.com/news/norton-healthcare-network-update/ (accessed via Wayback Machine, https://web.archive.org/web/20230511225626/https://nortonhealthcare.com/news/norton-healthcare-network-update/, on July 7, 2023), **attached as Exhibit B.**
[19] *Id.*
[20] *Id.*

disclose whether the personal information and PHI of patients and employees was impacted in the breach.

44. On May 22, 2023, Norton updated their website notice ("May 22, 2023 Norton Healthcare Network Update") to expound that on May 9, 2023, their information services team not only noticed suspicious network activity, but was, "alerted to the receipt of a faxed communication containing threats and demands. As this matter is under investigation, we are unable to share specifics of the message." [21]

45. While Defendants' May 22, 2023 Norton Healthcare Network Update still did not disclose whether patients' and employees' PHI was compromised or unauthorizedly accessed in the Data Breach, it went onto warn that, "[c]yber security experts recommend that you keep a close eye on your bank and investment accounts, as well as regularly change your account passwords [and] [i]f you suspect any unusual activity on your account, notify your banking institution."[22]

46. Defendants' May 22, 2023 Norton Healthcare Network Update too explained that, "[d]ue to the tremendous efforts of our Information Services team, our network was never out of our control. This bears repeating: At no point did an external force take control of or shut down our network. All of our facilities remain open and patient care continues."[23]

47. On May 24, 2023, Norton updated the website notice ("May 24, 2023 Norton Healthcare Network Update").[24]

---

[21] Norton Healthcare, "May 22, 2023 Norton Healthcare Network Update," available via Wayback Machine at https://web.archive.org/web/20230523115635/https://nortonhealthcare.com/news/norton-healthcare-network-update/ (last acc. July 7, 2023) and **attached as Exhibit C.**

[22] *Id.*

[23] *Id.*

[24] Norton Healthcare, "May 24 Norton Healthcare Network Update," available at https://nortonhealthcare.com/news/norton-healthcare-network-update/?fbclid=IwAR3Hrjn-m1f4oCOUmikmxIMuhcEDnDk0MEfQrWgDpcms9FGsplNKTYGKkNU (last acc. July 7, 2023), **attached as Exhibit D.**

48. Despite Norton's prior representations that their medical facilities remained open, even at two (2) weeks following the Data Breach on May 24, 2023, patients experienced cancelled medical procedures and surgeries, and delays in receiving their medications as a result.[25]

49. Moreover, as of that date, "…peace of mind [was] another factor that has been disrupted for patients. Norton has been unable to say whether or not patient or employee information was compromised."[26]

50. On or about May 25, 2023, cybercriminals, "Alphv," or "BlackCat" a "Ransomware as a Service (RaaS) group," based out of Russia posted a notice on the internet taking responsibility for the May 9, 2023 cyberattack, making clear it was a ransomware attack, and stating that, "[w]e have provided more than enough time to NORTON's Executive and Board Members but they're failed to show bravery to protect privacy of their clients and employees. Simply, They failed to protect confidential data and They're making false statements in the recent news and lying people that they've received fax and…" [27]

51. Based on the cybercriminal's announcement, the data and PHI unauthorizedly disclosed in the Data Breach included, "patients [sic] data, privacy photos, clinical imaging data," "images belong to all patients and millions of SSN records.. and 25k Employees![,]" "4.7 terabytes of data." In the announcement, cybercriminals also stated that they had included a selection of the sample of data accessed.

52. According to DataBreaches.net, the samples of information accessed in the Data

[25] *See* WDRB, "Patients remain frustrated 2 weeks after initial cyberattack on Norton Healthcare system," May 24, 2023, available at https://www.wdrb.com/news/patients-remain-frustrated-2-weeks-after-initial-cyberattack-on-norton-healthcare-system/article_acb720fc-faa3-11ed-9c77-333c2f0164dc.html (last acc. Oct. 31, 2023).
[26] *Id*.
[27] BlackCat/ALPHV Ransomware Victim: Norton Healthcare, available at https://www.redpacketsecurity.com/alphv-ransomware-victim-norton-healthcare/ (last accessed July 7, 2023)

Breach of which cybercriminals posted samples included "personal and sensitive information of patients. It also includes other types of files including images of checks and bank statements, and files with employees' personnel information such as name, date of birth, and Social Security number.[28]

53. Alphv posted its May 25, 2023 blog entry to the Dark Web, including 86 image files containing samples of the data and PHI exfiltrated in the Data Breach, including financial records, banking records, employee records and patient records that were clearly associated with Norton, including:

a. Patient data such as names, addresses, telephone numbers, Social Security numbers, dates of birth, diagnostic data, treatment data, insurance data, prescription data, imaging data, and lab data;

b. Employee data such as names, addresses, phone numbers, Social Security numbers, banking routing and account numbers, driver's licenses, and dates of birth.

c. Vendor data including names and Social Security numbers.

d. Also available were Credit card numbers with names, addresses, and CVV codes.

54. There is no question that Plaintiffs' and the Class Members' PHI, and sensitive patient and employee records, documents, and financial information was exfiltrated by cybercriminals, Alphv, in the Data Breach, and posted to the Dark Web, based on the admissions of the cybercriminals themselves and the samples of data they posted.

[28] DataBreaches.net, "Norton Healthcare didn't call it a ransomware attack. Then BlackCat claimed responsibility for it," May 25, 2023, available at https://www.databreaches.net/norton-healthcare-didnt-call-it-a-ransomware-attack-then-blackcat-claimed-responsibility-for-it/ (last acc. Oct. 31, 2023).

55. On information and belief, the information and PHI unauthorizedly disclosed in Norton's Data Breach, and posted to the Dark Web, included Plaintiffs' and the Class Members' sensitive medical information and records, full names, addresses, telephone numbers, Social Security numbers, dates of birth, medical information such as diagnostic data, treatment data, insurance data, prescription data, imaging data, and lab data; banking routing and account numbers, driver's licenses, and credit card numbers with names, addresses, and CVV codes.

56. On information and belief, the PHI unauthorizedly disclosed in the Data Breach was used for fraudulent purposes or posted to the Dark Web even before May 25, 2023, based on the damages caused to Plaintiffs and the Class Members, as follows below.

57. Even as of July 2023, 2-months following the Data Breach, patients continued to experience significant disruption in receiving medical services and test results from Norton as a result—as reported by WDRB, one patient, Audrey Frazier, who received a mammogram on the day of the cyberattack, May 9, 2023, and had "a lot of abnormal mammograms and several biopsies," only received her test results in July 2023 after contacting her physicians repeatedly.[29]

58. On information and belief, Norton chose not to pay the ransom to Alphv/Blackcat, and now the PHI unauthorizedly disclosed to and exfiltrated by these cybercriminals in the Data Breach—totaling 4.7 terabytes of data—has been posted to the Dark Web and is in the hands of the Russian ransomware attackers.

59. Norton did not have adequate security protocols to prevent, detect, and stop the cybercriminals from committing the cyberattack, a ransomware attack, and accessing the

[29] *See* WDRB, Valerie Chinn, "After 2-month wait for mammogram results, Louisville woman says Norton patients are 'due an explanation,'" July 19, 2023, avail. at https://www.wdrb.com/wdrb-investigates/after-2-month-wait-for-mammogram-results-louisville-woman-says-norton-patients-are-due-an/article_2d509ef8-24c2-11ee-8577-2736f2ae6747.html (last acc. Oct. 31, 2023).

voluminous PHI of Plaintiffs and the proposed Class Members which Norton stored on their systems, in the Data Breach.

60. Norton failed to adequately train their employees on reasonable cybersecurity protocols and failed to implement reasonable security measures, causing it to lose control over current and former patients' and employees' PHI in the Data Breach.

61. Norton has failed to take prompt and adequate remedial measures to prevent further disclosures of Plaintiffs' and the Class Members' PHI in the Data Breach.

62. Defendants have failed to notify affected patients and employees, including Plaintiffs and the proposed Class Members, of the Data Breach.

63. Defendants further concealed the nature of the Data Breach in that they did not explain who breached Norton's systems, the nature of the attack (e.g., a ransomware cyberattack), or the details of how the Data Breach occurred (e.g., whether systems were encrypted, and/or if a monetary ransom was paid), or whose information and PHI was compromised in the Data Breach, and that the PHI had been posted to the Dark Web, once known.

64. Defendants' tortious conduct and breach of contractual obligations, as explained hereinafter, are evidenced by their failure to recognize the Data Breach until cybercriminals had already accessed the data, meaning Norton had no effective means to detect and prevent attempted data breaches.

65. On information and belief, as a result of the Data Breach which Defendants permitted to occur by virtue of their inadequate data security practices, Plaintiffs and the proposed Class Members have suffered identity theft and fraudulent charges, have been forced to expend significant times and effort to remediate the consequences of the breach, and have been caused anxiety and emotional distress; as well as a lifetime risk of identity theft, as it includes sensitive

information that cannot be changed, like their dates of birth and Social Security numbers.

C. Plaintiffs' Experiences

Plaintiff Berthold

66. For the past ten (10) years, approximately, Plaintiff Berthold has been a patient of Defendants.

67. As a material condition of receiving medical services from Norton, Plaintiff Berthold was required to provide Defendants with her Private Information, including her full name, date of birth, address, Social Security Number, and other information including financial information, such as her credit card information.

68. Plaintiff Berthold became aware of the Data Breach to Norton's systems based upon Defendants' "May 24 Norton Healthcare Network Update," posted online, Exhibit D.

69. Upon information and belief, Plaintiff Berthold's Private Information, including but not limited to her full name, Social Security Number, and financial account information was unauthorizedly disclosed and compromised in the Data Breach.

70. As a direct result of the Data Breach Defendants permitted to occur, Plaintiff Berthold has suffered identity fraud and fraudulent misuse of her Private Information, and fraudulent charges, as follows:

a. Multiple fraudulent charges to Door Dash on May 16, 2023, May 17th, May 18th, and May 19th;

b. Fraudulent charges on May 16th and 17th to her Amazon Kindle account.

Both fraudulently charged accounts are connected to Plaintiff Berthold's credit card which she used to pay Norton for medical treatment received.

71. Further, Plaintiff Berthold has spent considerable time and effort attempting to

remediate the harmful effects of these fraudulent charges, including being forced to contact her financial institutions, Door Dash, and Amazon to remediate the charges and to prevent further fraudulent withdraws and damage, as well as time and effort to monitor her accounts to protect herself from additional identity theft.

72. Plaintiff Berthold fears for her personal financial security and uncertainty over the fraudulent charges and devastating impact on her finances caused by the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

73. Plaintiff Berthold was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive Private Information and the harm caused by the Data Breach. She was also outraged that Norton has yet to notify her of the Data Breach. Considering the extreme harm caused by the Data Breach.

74. As a result of Norton's Data Breach, Plaintiff Berthold faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like her date of birth and Social Security number.

75. In light of the foregoing fraudulent activity, it is obvious that Plaintiff Berthold's Private Information was disclosed to cybercriminals in the Data Breach to Norton's systems and is now publicly available, including on the Dark Web, for sale and for criminal and fraudulent use, resulting in injury and damages.

Plaintiff D'Spain

76. Plaintiff D'Spain was an employee of Norton Healthcare beginning in the 1980s and until 2007, approximately, as a nurse and then case manager.

77. As a material condition of employment, Norton required Plaintiff D'Spain to provide Defendants with her PHI, including her full name, date of birth, address, Social Security Number, and other information including financial information, which Defendants stored in their computer network systems.

78. To her knowledge, prior to this Data Breach, Plaintiff D'Spain has never been involved in a data security incident in which her PHI was unauthorizedly disclosed, and she is careful with her sensitive PHI to prevent unauthorized disclosure.

79. Plaintiff D'Spain became aware of the Data Breach to Norton's systems based upon media reports.

80. Upon information and belief, Plaintiff D'Spain's PHI was unauthorizedly disclosed and compromised in the Data Breach, as evidenced by the fraudulent activity using her identity following the Data Breach.

81. As a direct result of the Data Breach which Defendants permitted to occur, Plaintiff D'Spain has suffered and will suffer injury and damages, including fraudulent activity, charges, and purchases or applications, as well as lost time to mitigate the effects of the Data Breach, and anxiety and emotional distress:

a. Following the May 9, 2023 Data Breach, and the cybercriminals posts of PHI to the Dark Web, on or around June 1, 2023, Plaintiff D'Spain's debit card associated with Chase Bank experienced fraudulent activity, which the bank was able to stop;

b. On June 5, 2023 Plaintiff D'Spain received a telephone call from a local automobile dealer, Montgomery Chevrolet, stating that her new car was ready, and disclosing her husband's name, when she had not purchased a

new car.

c. On June 23, 2023, Plaintiff D'Spain received an alert that she was approved for a $10,000.00 loan, evidencing a fraudulent loan application or other fraudulent misuse of her identity.

82. Plaintiff D'Spain has spent, and will be required to expend, considerable time and effort attempting to remediate the harmful effects of the Data Breach, including to dispute and address fraudulent activity with her financial institutions and other businesses, as well as time and effort in the future to monitor her accounts and to protect herself from additional identity theft.

83. Plaintiff D'Spain fears for her personal financial security and uncertainty over the PHI disclosed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

84. Plaintiff D'Spain was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PHI and the harm caused by the Data Breach. She was also outraged that Norton has yet to notify her of the Data Breach.

85. As a result of Norton's Data Breach, Plaintiff D'Spain faces a lifetime risk of identity theft, as, on information and belief, it includes sensitive information that cannot be changed, like her date of birth and Social Security number.

86. Considering the above fraudulent activity following the Data Breach, when Plaintiff D'Spain has never been the victim of a prior data breach, it is obvious that Plaintiff D'Spain's PHI was disclosed to cybercriminals in the Data Breach to Norton's systems and is now publicly available, including on the Dark Web, for sale and for criminal and fraudulent use, resulting in

injury and damages.

Plaintiff Malone

87. Plaintiff Malone was an employee of Norton Healthcare, Inc. from 2015 to 2022, and a longtime patient of Defendants.

88. As a material condition of employment and of receiving medical services, Norton required Plaintiff Malone to provide Defendants with her PHI, including her full name, date of birth, address, Social Security Number, and other information including her telephone number, email address, marital status, employers with contact information, primary and secondary insurance policy holders' names, demographic information, driver's license or state or federal identification, medical information and medical history, insurance information and coverage, as well as financial information, which Defendants stored in their computer network systems.

89. To her knowledge, prior to this Data Breach, Plaintiff Malone has never been involved in a data security incident in which her PHI was unauthorizedly disclosed, and she is careful with her sensitive PHI to prevent unauthorized disclosure.

90. Plaintiff Malone became aware of the Data Breach to Norton's systems based upon media reports and Defendants' online May 2023 network updates.

91. Upon information and belief, Plaintiff Malone's PHI was unauthorizedly disclosed and compromised in the Data Breach, as evidenced by her being informed in June 2023 that her PHI, including her Social Security Number and credit card information, was found on the Dark Web, as well as by the fraudulent activity using her identity following the Data Breach.

92. As a direct result of the Data Breach which Defendants permitted to occur, Plaintiff Malone has suffered and will suffer injury and damages, including fraudulent activity, charges, and fraudulent loans or applications, as well as lost time to mitigate the effects of the Data Breach, and

anxiety and emotional distress:

a. In June 2023, Plaintiff Malone was contacted by her bank about a suspicious charge being attempted for $1500.00, which she was able to intercept and her bank did not allow to go through. She was required to spend about an hour time trying to resolve this fraudulent activity, and required to get new credit/debit cards to protect her financial well-being as well as her credit rating;

b. In addition, for approximately the past few months, Plaintiff Malone has been receiving letters and calls about car payments that she does not owe. Upon further investigation, she found out someone took out a CarMax loan for a 2011 Dodge Charger in her name with her Social Security Number. The person who made the unauthorized transaction did not make any payments on the vehicle. Plaintiff Malone has already spent hours trying to resolve this fraudulent loan and the damage it has caused on her credit.

c. As a result of the identity thief purchasing the 2011 Dodge Charger, Plaintiff Malone's credit has been adversely affected. She has been trying to move into a new apartment, but she is being turned away from leasing offices due to the effects of fraudulent purchase of the vehicle and nonpayment on her credit report.

d. Plaintiff Malone now also receives multiple spam calls and texts every day, at the same address and phone numbers she provided to Norton for her employment and healthcare.

e. Plaintiff Malone reasonably believes these fraudulent activities are directly

related to the Data Breach.

93. Plaintiff Malone has spent, and will be required to expend, considerable time and effort attempting to remediate the harmful effects of the Data Breach, including to dispute and address fraudulent activity with her financial institutions and other businesses, two (2) hours per week monitoring her financial accounts, as well as time and effort in the future to monitor her accounts and to protect herself from additional identity theft.

94. Plaintiff Malone fears for her personal financial security and uncertainty over the PHI disclosed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

95. Plaintiff Malone was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PHI and the harm caused by the Data Breach. She was also outraged that Norton has yet to notify her of the Data Breach.

96. As a result of Norton's Data Breach, Plaintiff Malone faces a lifetime risk of identity theft, as, on information and belief, it includes sensitive information that cannot be changed, like her date of birth and Social Security number.

97. Considering the above fraudulent activity following the Data Breach, when Plaintiff Malone has never been the victim of a prior data breach, it is obvious that her PHI was disclosed to cybercriminals in the Data Breach to Norton's systems and is now publicly available, including on the Dark Web, for sale and for criminal and fraudulent use, resulting in injury and damages.

D. This Data Breach was Foreseeable by Defendants.

98. Plaintiffs and the proposed Class Members provided their PHI to Norton with the

reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendants put Plaintiffs and Class Members at risk of identity theft, financial fraud, and other harms.

99. Defendants tortiously failed to take the necessary precautions required to safeguard and protect the PHI of Plaintiffs and the Class Members from unauthorized disclosure. Defendants' actions represent a flagrant disregard of Plaintiffs' and the other Class Members' rights.

100. Plaintiffs and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing PHI and the critical importance of providing adequate security for that information.

101. In fact, as early as May 17, 2017, Norton was acknowledging the high risk of cyberattacks in an article prepared for its patients called "How to Protect Your Personal Health Information."[30] In the article, Norton lists things patients can do to protect themselves, but also tells how it is keeping patient information safe: "Many safeguards are in place to ensure only the people who need your health information have access to it. Patient information is protected through many layers of passwords, encryption and technical safeguards. 'Our priority within the information services department is the protection of Norton Healthcare patient and employee data," said Steve Ready, system vice president of information services and chief information officer. "We continue to take the necessary measures to ensure both our technical and informational resources are secured.'"[31]

[30] https://nortonhealthcare.com/news/7-tips-for-personal-cybersecurity/ (last accessed November 16, 2023).
[31] Id.

102. Moreover, cyber-attacks against healthcare organizations such as Defendants are targeted and frequent. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors…"[32]

103. According to the Identity Theft Resource Center's (ITRC) January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[33]

104. According to the ITRC's January 2023 report for 2022, "[t]he number of publicly reported data compromises in the U.S. totaled 1,802 in 2022. This represents the second highest number of data events in a single year and just 60 events short of matching 2021's all-time high number of data compromises."[34] In 2022, there were approximately 422 million individuals affected by cyberattacks.[35]

105. Moreover, of the 1,802 data breaches in 2022, ITRC reported that 1,560 involved compromised names, 1,143 involved compromised of Social Security Numbers, 633 involved

---

[32] HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, *2019 HIMSS Cybersecurity Survey*, available at https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last accessed July 7, 2023).

[33] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Apr. 14, 2023).

[34] Identity Theft Resource Center, 2022 Data Breach Report, available at https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, pg. 7 (last acc. Jul. 3, 2023).

[35] *See Id*., pg. 2.

compromised dates of birth, and 443 involved bank account numbers—similar to the types of PII unauthorized disclosed in this Data Breach.[36]

106. In 2022, there were 161 data security compromises in the healthcare industry, affecting 11,830,303 victims.[37]

107. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Norton. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[38]

108. As of 2022, "[t]he cost of a breach in the healthcare industry went up 42% since 2020. For the 12th year in a row, healthcare had the highest average data breach cost of any industry." The average total cost of a breach in the healthcare industry is $10.10 million.[39]

109. Furthermore, Defendants were aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

110. PHI is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

111. PHI can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

112. Given the nature of the Data Breach, it was foreseeable that the compromised PHI

---

[36] *Id*., pg. 6.
[37] *Id*., pg. 31.
[38] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. July 7, 2023).
[39] *Id*.

could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess the Class Members' PHI can easily obtain Class Members' tax returns or open fraudulent credit card accounts in the Class Members' names.

E. Norton Failed to Comply with FTC Guidelines

113. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

114. In 2016, the FTC updated its publication, *Protecting PHI: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PHI that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[40]

115. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security

[40] *See* Federal Trade Commission, October 2016, "Protecting PHI: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).

measures.[41]

116. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

117. These FTC enforcement actions include actions against entities failing to safeguard PHI such as Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

118. Norton failed to properly implement basic data security practices widely known throughout the industry. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

119. Defendants were at all times fully aware of their obligations to protect the PHI of their patients and employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

F. Norton Fails to Comply with Industry Standards

120. As shown above, experts studying cyber security routinely identify organizations holding PHI as being particularly vulnerable to cyber-attacks because of the value of the

[41] *See id*.

information they collect and maintain. As of 2022, ransomware breaches like that which occurred here had grown by 41% in the last year and cost on average $4.54 million dollars.[42]

121. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[43]

122. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.

[42] IBM, "Cost of a Data Breach Report 2022," available at https://www.ibm.com/reports/data-breach (last acc. July 7, 2023), pg. 6.
[43] *See* https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Apr. 14, 2023).

- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[44]

123. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to guard against ransomware attacks.[45]

124. Upon information and belief, Norton failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as other industry standards for protecting Plaintiffs' and the proposed Class Members' PHI, resulting in the Data Breach.

G. The Data Breach Caused Plaintiffs and the Class Members Injury and Damages

125. On information and belief, Plaintiffs and proposed Class Members have suffered injury and damages from the misuse of their PHI that can be directly traced to Norton and the Data Breach, that has occurred, is ongoing, and/or imminently will occur.

126. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiffs' and the proposed Class Members' PHI, which is now been posted to the Dark Web,

[44] Understanding The NIST Cybersecurity Framework, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).
[45] Cybersecurity & Infrastructure Security Agency, April 11, 2019 (rev. Sept. 2, 2021) available at https://www.cisa.gov/news-events/news/protecting-against-ransomware (last acc. Apr. 14, 2023).

and is being used for fraudulent purposes and/or has been sold for such purposes, causing widespread injury and damages.

127. The ramifications of Norton's failure to keep Plaintiffs' and the Class's PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

128. Because Norton failed to prevent the Data Breach, Plaintiffs and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and the Class Members have suffered, are at an increased risk of suffering, or will imminently suffer:

a. Fraudulent misuse of PHI, and fraudulent charges or attempted fraudulent charges;

a. Fraudulent loan applications and fraudulent loans;

b. Worsened credit scores, and lost opportunities as a result, including being denied apartments and housing;

c. Spam telephone calls and texts;

d. The loss of the opportunity to control how PHI is used;

e. The diminution in value of their PHI;

f. The compromise and continuing publication of their PHI;

g. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

h. Lost opportunity costs and lost wages associated with the time and effort

expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; contacting financial institutions to dispute fraudulent charges or attempted fraudulent charges, to cancel and reissue credit and debit cards, and addressing their inability to withdraw funds linked to compromised accounts; disputing other fraudulent activities such as loans; placing "freezes" and "alerts" with credit reporting agencies; resetting automatic billing and payment instructions from compromised credit and debit cards to new ones; and closely monitoring accounts for fraudulent activity that has already occurred and to prevent future fraudulent activity caused by the Data Breach;

i. Delay in receipt of tax refund monies;

j. Unauthorized use of stolen PHI;

k. Anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever; and,

l. The continued risk to their PHI, which remains in the possession of Norton and is subject to further breaches so long as Norton fails to undertake the appropriate measures to protect the PHI in their possession.

129. Furthermore, the Data Breach has placed Plaintiffs and the proposed Class Members at an increased risk of fraud and identity theft.

130. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax

refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[46]

131. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[47]

132. Identity thieves use stolen PHI such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

133. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

134. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's PHI to police during an arrest—resulting in an arrest warrant being issued in the victim's

[46] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 27, 2023).
[47] *See* https://www.identitytheft.gov/Steps (last visited September 1, 2021).

name.

135. According to the ITRC's 2022 Data Breach Report, "there has been a dramatic increase in identity scams and fraud where cybercriminals impersonate an individual using stolen data and/or information gleaned from social media accounts to apply for government benefits and to open new financial and non-financial accounts."[48] While this can mean that, "there are generally fewer victims of data breaches. […] the financial impact is likely higher and the time to remediate the effects of the identity misuse is longer."[49]

136. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated. [50]

137. Additionally, according to the ITRC, in 2022, "[d]ata breach notices suddenly lacked detail, resulting in increased risk for individuals and businesses as well as uncertainty about the true number of data breaches and victims."[51]

138. Here, Norton has refused to notify affected victims of the Data Breach, preventing

---

[48] Identity Theft Resource Center, 2022 Data Breach Report, available at https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, pg. 8.
[49] *Id*.
[50] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 27, 2023).
[51] Identity Theft Resource Center, 2022 Data Breach Report, available at https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, pg. 8.

them from taking appropriate measures to mitigate the harms caused by the Data Breach.

139. What's more, theft of PHI is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PHI/PHI is a valuable property right.[52]

140. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PHI has considerable market value.

141. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when PHI and/or financial information is stolen and when it is used.

142. Thus, Plaintiffs and the Class Members must vigilantly monitor their financial and medical accounts for many years to come.

143. Social Security numbers are among the worst kind of PHI 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.[53]

144. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may

---

[52] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PHI") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PHI, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[53] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023).

go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[54] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

145. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he 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."[55]

146. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[56] Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[57]

147. Accordingly, the Data Breach has caused Plaintiffs and the proposed Class

---

[54] *See id.*

[55] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

[56] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited September 1, 2021).

[57] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed September 1, 2021).

Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the identity fraud and criminal fraudulent activity, fraudulent charges, theft of monies, and attendant costs, lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

148. Norton knew or should have known of these harms which would be caused by the Data Breach they permitted to occur, and strengthened their data systems accordingly.

CLASS ALLEGATIONS

149. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

150. Plaintiffs bring this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to CR 23.01, *et seq*.

151. Plaintiffs propose the following Class definition(s), subject to amendment based on information obtained through discovery:

> **All persons whose PHI was compromised as a result of the Data Breach experienced by Defendants on or about May 9, 2023 as announced by Norton and to whom Defendants were required to provide direct notice.**

152. Excluded from the Class are Defendants' officers, directors; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

153. Plaintiffs reserve the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

154. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of Class Members' claims on a class-wide basis using the same

evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

155. This action satisfies the requirements for a class action under CR 23.01(a)-(d) and CR 23.02(c), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

156. **Numerosity, CR 23.01(a).** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, potentially millions of Defendants' patients' PHI and at least 25,000 employees' PHI was compromised in the Data Breach. Such information is readily ascertainable from Defendants' records.

157. **Commonality and Predominance, CR 23.01(b), CR 23.02(c).** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PHI;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

d. Whether Defendants' data security systems prior to and during the Data

Breach were consistent with industry standards;

e. Whether computer hackers obtained Plaintiffs' and Class Members' PHI in the Data Breach;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether Plaintiffs and the Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

h. Whether Defendants breached the covenant of good faith and fair dealing implied in their contracts with Plaintiffs and Class Members;

i. Whether Plaintiffs and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

158. **Typicality, CR 23.01(c).** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs' allegations, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendants.

159. **Adequacy, CR 23.01(d).** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

160. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data—PHI—was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and

desirable advantages of judicial economy.

161. **Superiority, CR 23.02.** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendants has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendants, will

increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendants.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Norton's patients and employees, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendants' records, such that direct notice to the Class Members would be appropriate.

162. In addition, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis under CR 23.02(b).

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

164. Defendants required Plaintiffs and the Class Members to submit private, confidential PHI to it, as a condition of receiving medical treatment or as a material condition of

employment with Defendants.

165. Plaintiffs and the Class Members are individuals who provided certain PHI to Defendants including but not limited to their full names, addresses, telephone numbers, Social Security numbers, dates of birth, medical information such as diagnostic data, treatment data, insurance data, prescription data, imaging data, and lab data; banking routing and account numbers, driver's licenses, and credit card numbers with names, addresses, and CVV codes.

166. Defendants had full knowledge of the sensitivity of the PHI to which they were entrusted, and the types of harm that Plaintiffs and the Class Members could and would suffer if the PHI was wrongfully disclosed to unauthorized persons. Defendants had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information.

167. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their data in Defendants' possession.

168. By collecting and storing this data in their computer systems, Defendants had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect if that PHI was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

169. Defendants owed a duty of care to Plaintiffs and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected PHI.

170. Defendants' duty of care to use reasonable security measures arose as a result of

the special relationship that existed between Defendants and their patients and employees, which is recognized by the common law, and applicable laws and regulations including the FTC Act. Defendants were able to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

171. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

172. Defendants' duty to use reasonable care in protecting confidential data and PHI arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PHI.

173. Defendants breached their duties, and were negligent, by acts of omission or commission, by failing to use reasonable measures to protect the Plaintiffs' and Class Members' PHI. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' PHI;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of their networks and systems;

d. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiffs' and Class Members' PHI;

f. Failing to timely notify Plaintiffs and Class Members about the Data Breach

so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

174. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiffs' and Class Members' PHI would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

175. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PHI would result in one or more types of injuries to them.

176. As a direct and proximate result of Defendants' negligence set forth in the preceding paragraphs, Plaintiffs and Class Members have suffered injury and damages as set forth herein, including fraudulent misuse of PHI and fraudulent activity and charges; loss of the opportunity to control how their PHI is used; diminution in value of their PHI; compromise and continuing publication of their PHI; and are entitled to compensatory damages suffered as a result of the Data Breach, as well as punitive damages.

177. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately notify all affected persons of the Data Breach; and (iv) provide adequate credit monitoring to all Class Members.

178. Pursuant to CR. 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

179. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

180. As a condition of receiving medical care from Defendants, or as a condition of employment, Plaintiffs and the Class provided their PHI to Defendants, and, with patients, paid compensation for the treatment received. Through their course of conduct, Plaintiffs, and Class Members entered into implied contracts for employment or for medical services with Defendants, and that Defendants would deal with them fairly and in good faith, as well as implied contracts for the Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PHI entrusted to Defendants.

181. Specifically, Plaintiffs and the Class Members entered into valid and enforceable implied contracts with Defendants when they first accepted employment or first utilized Defendants' medical services, and when they first provided Norton with their PHI and payment to effectuate these purposes.

182. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Defendants included Defendants' promise to protect nonpublic PHI given to Defendants or that Defendants created on their own from unauthorized disclosures. Plaintiffs and Class Members provided this PHI in reliance of that promise.

183. Defendants solicited and invited Plaintiffs and Class Members to provide their PHI as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their PHI to Defendants as a condition of employment or as a condition of receiving medical services.

184. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with industry standards as well as relevant laws and regulations, including the FTC Act.

185. Plaintiffs and Class Members who rendered labor to Defendants in connection with employment or who paid money to Defendants for medical services, and who provided their PHI to Defendants, reasonably believed and expected that Defendants would adequately employ adequate data security to protect that PHI. Defendants failed to do so.

186. Under the implied contracts, Defendants promised and were obligated to: (a) pay compensation in connection with the employment relationship, or provide medical services to patients, to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' PHI: (i) provided to obtain such employment and/or treatment; and/or (ii) created in connection therewith. In exchange, Plaintiffs and Class Members agreed to render labor or pay money for these services and to turn over their PHI.

187. Both the provision of employment or medical treatment, and the protection of Plaintiffs' and Class Members' PHI, were material aspects of these implied contracts.

188. The implied contracts for employment or the rendering of medical treatment—contracts that include contractual obligations to maintain the privacy of Plaintiffs' and Class Members' PHI—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' Notice of Privacy Practices with patients as described in the preceding paragraphs.

189. Defendants' representations, including, but not limited to the representations found in their Notice of Privacy Practices, described in the preceding paragraphs, memorialize and embody an implied contractual obligation requiring Defendants to implement data security

adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PHI.

190. Plaintiffs and the Class Members as employees or patients of Defendants value their privacy, the privacy of their dependents, and the ability to keep their PHI private. To employees and patients such as Plaintiffs and the Class Members, Defendants' practices that do not adhere to industry-standard data security protocols to protect PHI render the employment or medical services fundamentally less useful and less valuable than that which adheres to industry-standard data security.

191. Plaintiffs and Class Members would not have entrusted their PHI to Defendants and entered into these implied contracts with Defendants without an understanding that their PHI would be safeguarded and protected, or entrusted their PHI to Defendants, in the absence of their implied promise to monitor their computer systems and networks to ensure that PHI was not disclosed to unauthorized parties and exposed to the public as occurred in the Data Breach.

192. A meeting of the minds occurred when Plaintiffs and the Class Members agreed to, and did, provide their PHI to Defendants and paid for employment or to receive medical services from Defendants, for, amongst other things, (a) the provision of such employment or treatment and (b) the protection of their PHI.

193. Plaintiffs and the Class Members performed their obligations under the contracts when they rendered labor to Defendants or paid for medical services and provided their PHI to Defendants.

194. Defendants materially breached their contractual obligations to protect the nonpublic PHI Defendants required and gathered when the information was unauthorizedly disclosed in the Data Breach.

195. Defendants materially breached their contractual obligations to deal fairly and in

good faith with Plaintiffs and the Class Members when they failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

196. Defendants materially breached the terms of their implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendants did not maintain the privacy of Plaintiffs' and the Class Members' PHI. Specifically, Defendants did not comply with industry standards, the standards of conduct embodied in statutes like Section 5 of the FTC Act, or otherwise protect Plaintiffs' and the Class Members' PHI, as set forth above.

197. The Data Breach was a reasonably foreseeable consequence of Defendants' conduct, by acts of omission or commission, in breach of these contracts.

198. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains, and instead received employment or medical services with Defendants that were of a diminished value compared to those described in the contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services and/or employment with data security protection they paid for and that which they received.

199. Had Defendants disclosed that their security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have rendered labor in connection with employment or purchased medical services from Defendants.

200. As a direct and proximate result of the Data Breach, Plaintiffs and the Class Members have suffered injury and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they had struck with Defendants.

201. Plaintiffs and the Class Members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

202. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately notify all affected persons of the Data Breach; and (iv) provide adequate credit monitoring to all Class Members.

203. Pursuant to CR 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

204. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

205. This claim is pleaded in the alternative to the claim of breach of implied contract (Count II).

206. Plaintiffs and members of the Class conferred benefits upon Defendants in the form of labor rendered in connection with employment or payments for medical services. Also, Defendants received additional benefits from receiving the PHI of Plaintiffs and Class Members—such data is used to facilitate both payment and the provision of services.

207. Defendants appreciated or knew of these benefits that they received. And under principles of equity and good conscience, this court should not allow Defendants to retain the full value of these benefits—specifically, the payments, value of labor, and PHI of Plaintiffs and members of the Class.

208. After all, Defendants failed to adequately protect Plaintiffs' and Class Members'

PHI. And if such inadequacies were known, then Plaintiffs and the members of the Class would never have conferred labor or payment to Defendants, nor disclosed their PHI.

209. Defendants should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all funds that were unlawfully or inequitably gained despite Defendants' misconduct and the resulting Data Breach.

210. Pursuant to CR 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

COUNT IV
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

211. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

212. Plaintiffs and the Class Members had a legitimate expectation of privacy to their PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

213. Defendants owed a duty to their current and former patients and employees, including Plaintiff and the Class Members, to keep their PHI confidential.

214. Defendants failed to protect said PHI and exposed the PHI of Plaintiffs and the Class Members to unauthorized persons which is now publicly available, including on the dark web, and being fraudulently misused.

215. Defendants allowed unauthorized third parties access to and examination of the PHI of Plaintiffs and the Class Members, by way of Defendants' failure to protect the PHI.

216. The unauthorized release to, custody of, and examination by unauthorized third parties of the PHI of Plaintiffs and the Class Members is highly offensive to a reasonable person.

217. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class Members disclosed their PHI to Defendants as a condition of employment with Defendants or as a condition of receiving medical services, but privately with an intention that the PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

218. The Data Breach constitutes an intentional or reckless interference by Defendants with Plaintiffs' and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

219. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they had actual knowledge that their information security practices were inadequate and insufficient.

220. Defendants acted with reckless disregard for Plaintiffs' and Class Members' privacy when they allowed improper access to their systems containing Plaintiffs' and Class Members' PHI.

221. Defendants were aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' PHI.

222. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class Members.

223. Defendants communicated Plaintiffs' and Class Members' PHI to the public at

large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge, including but publication on the Dark Web, as evidenced by the criminal and fraudulent identity theft and fraud suffered by Plaintiff and the Class Members.

224. Defendants gave publicity to a matter concerning Plaintiffs' and Class Members' private lives by exposing their PHI to unauthorized third parties and now to the public on the Dark Web.

225. The disclosure of Plaintiffs' and Class Members' PHI would be highly offensive to a reasonable person, and is not of legitimate concern to the public.

226. As a direct and proximate result of Defendants' invasion of privacy set forth in the preceding paragraphs, Plaintiffs and Class Members have suffered injury and damages as set forth herein, including fraudulent misuse of PHI and fraudulent activity and charges; loss of the opportunity to control how their PHI is used; diminution in value of their PHI; compromise and continuing publication of their PHI; and are entitled to compensatory damages suffered as a result of the Data Breach, as well as punitive damages.

227. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the PHI maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class Members.

228. Pursuant to CR 8.01, the amount in controversy exceeds the minimum jurisdiction of the Jefferson Circuit Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, ABBY BERTHOLD, CHARLOTTE D'SPAIN, and LANISHA MALONE, on behalf of themselves, and all others similarly situated, pray for judgment as follows:

A. Trial by jury;

B. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

C. Awarding Plaintiffs and the Class damages that include applicable compensatory damages, exemplary, consequential, and punitive damages, as allowed by law;

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

E. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

F. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

G. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the transmitted PHI;

H. Awarding attorneys' fees and costs, as allowed by law;

I. Awarding prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

K. Any and all such relief to which Plaintiffs and the Class are entitled.

Dated: November 21, 2023

Respectfully submitted,

/s/ J. Gerard Stranch, IV

J. Gerard Stranch, IV (*Pro Hac Vice*)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gstranch@stranchlaw.com

Lynn A. Toops, *(Pro Hac Vice)*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com

Interim Class Counsel

/s/ Andrew E. Mize

Andrew E. Mize (Ky. Bar No. 94453)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
amize@stranchlaw.com

Mary Kate Dugan (*Pro Hac Vice* forthcoming)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
mdugan@cohenandmalad.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775
(608) 509-4423 (facsimile)
sam@turkestrauss.com

Tad Thomas (Ky. Bar No. 88577)
Julie Pahler (Ky. Bar No. 99449)
THOMAS LAW OFFICES
9418 Norton Commons Blvd., Suite 200

Louisville, Kentucky 40059
(502) 473-6540
tad@thomaslawoffices.com
Julie.Pahler@thomaslawoffices.com

Alexander Edmondson (Ky. Bar No. 88406)
EDMONDSON & ASSOCIATES LAW
28th West 5th
Covington, Kentucky 41011
(859) 491-4100
aedmondson@edmondsonlaw.com

Gary E. Mason (*Pro Hac Vice* forthcoming)
Lisa A. White (*Pro Hac Vice* forthcoming)
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
(202) 429-2290
gmason@masonllp.com
lwhite@masonllp.com

Counsel for Plaintiffs and the Class

CERTIFICATE OF SERVICE

It is hereby certified that on this 21st day of November 2023, a true and accurate copy of the foregoing was filed with the Clerk of the Jefferson Circuit Court via the Kentucky Court of Justice eFiling system, which will electronically serve the following:

Michael P. Abate, Esq.
Wm. R. (Rick) Adams, Esq.
KAPLAN JOHNSON ABATE & BIRD, LLP
710 W. Main St., 4th Floor
Louisville, Kentucky 40202
(502) 540-8280
mabate@kaplanjohnsonlaw.com

David Saunders, Esq. (*Pro Hac Vice)*
MCDERMOTT WILL & EMERY
444 W. Lake Street, Suite 4000
Chicago, Illinois 60606-0029
(312) 803-8305
dsaunders@mwe.com
Counsel for Defendants

/s/ Andrew E. Mize
Andrew E. Mize (Ky. Bar No. 94453)
Counsel for Plaintiffs and the Class

EXHIBIT A

HIPAA

Learn More

Request Appointment

SUBMENU

Notice of Privacy Practices

Effective date: April 14, 2003

Revised: July 22, 2007; Sept. 14, 2009; Aug. 30, 2011; Sept. 23, 2013; Nov. 1, 2016; June 30, 2021

This notice describes how medical information about you may be used and disclosed and how you can get access to this medical information. Please review it carefully.

For more information about Norton Healthcare's privacy policies, contact the Norton Healthcare Health Information Management Department at P.O. Box 35070, Louisville, KY 40232-5070 or **(502) 629-8766**, or call the Norton Healthcare Compliance Hotline at **(866) 264-4567**.

Who will follow this notice:

This notice describes Norton Healthcare's practices and those of:

- Any health care professional authorized to enter information into a patient's chart
- All departments and units within Norton Healthcare facilities
- Any member of a volunteer group that Norton Healthcare allows to help patients while they are in a Norton Healthcare facility
- All employees, staff and other Norton Healthcare facility personnel and participating members of the medical staffs
- Norton Healthcare hospitals, physician practices and any other owned or managed entities of Norton Healthcare

All these entities, sites and locations follow the terms of this notice. In addition, these entities, sites and locations may share with each other medical information related to patient treatment, payment or health care operations described in this notice and as otherwise permitted by law.

Norton Healthcare's pledge regarding medical information

We understand that medical information about the health of our patients is personal. We are committed to protecting patients' personal medical information. We create a record of the care and services patients receive at Norton Healthcare facilities. We need these records to provide patients with quality care and to comply with certain legal requirements.

This notice applies to patient care records generated or maintained by Norton Healthcare facilities, whether made by facility personnel or by a physician. A patient's private doctor may have different policies or notices about the use and disclosure of medical information created in the doctor's office or clinic.

This notice explains ways in which Norton Healthcare may use and disclose medical information about its patients. It also describes patients' rights with respect to their medical information.

Norton Healthcare is required by law to:

- Make sure medical information that identifies patients is kept private
- Give patients this notice of our legal duties and privacy practices with respect to patients' medical information
- Obtain an acknowledgment from each patient regarding receipt of this notice
- Follow the terms of the notice that are currently in effect
- Notify affected individuals following a breach of unsecured protected health information

How Norton Healthcare may use and disclose patients' medical information

The following categories describe different ways Norton Healthcare uses and discloses medical information. For each category of uses or disclosures, there is an explanation and examples. Not every use or disclosure in a category will be listed. However, all of the ways Norton Healthcare is permitted to use and disclose information will fall within one of these categories.

For treatment. Norton Healthcare may use medical information about patients to provide medical treatment or services. We may disclose medical information about patients to doctors, nurses, technicians, medical or health care professions students, or other facility personnel who are involved in care at a Norton Healthcare facility. For example, a doctor treating a patient for a broken leg may need to know if the patient has diabetes, because diabetes may slow the healing process. In addition, the doctor may need to tell the dietitian if a patient has diabetes so that appropriate meals can be arranged. Different departments of a hospital also may share medical information about patients in order to coordinate the different things patients need, such as prescriptions, lab work and X-rays. We also may disclose medical information about patients to people outside the hospital or to other facilities or persons who may be involved in a patient's medical care after discharge.

For payment. Norton Healthcare may use and disclose medical information about patients so that the treatment and services received may be billed to and payment may be collected from patients, an insurance company or another third party. For example, we may need to provide health plan information about a surgery received at the hospital so a patient's health plan will pay the hospital or reimburse the patient for the surgery. We also may inform a patient's health plan about a treatment he or she is going to receive to obtain prior approval or to determine whether the plan will cover the treatment.

For health care operations. Norton Healthcare may use and disclose medical information about patients for health care operations. These uses and disclosures are necessary to run our facilities and make sure that all of our patients receive quality care. For example, we may use medical information to review our treatment and services and to evaluate the performance of our staff in caring for patients or for accreditation or credentialing activities. We also may combine medical information about many hospital patients to decide what additional services the hospital should offer, what services are not needed and whether certain treatments are effective. We may disclose information to doctors, nurses, technicians, medical students and other hospital personnel for review and learning purposes.

Appointment reminders. Norton Healthcare may use and disclose medical information to remind patients of appointments for treatment or medical care at a Norton Healthcare facility.

Treatment alternatives. Norton Healthcare may use and disclose medical information to tell patients about or recommend possible treatment options or alternatives that may be of interest.

Health-related benefits and services. Norton Healthcare may use and disclose medical information to tell patients about our own health care-related products and services that may be of interest so long as certain conditions set by law are satisfied. These communications may include information to help patients manage and improve their health, schedules of upcoming classes and health screenings, and Norton Healthcare's magazine Get Healthy, among others. If patients do not want to receive this type of information, they can write to Norton Healthcare, Marketing & Communications, 224 E. Broadway, Third Floor, Mailbox M-46, Louisville, KY 40202.

Fundraising activities. Norton Healthcare may use medical information to contact patients in an effort to support Norton Healthcare facilities and programs through one of our two foundations. We may disclose medical information to a foundation related to Norton Healthcare or to a business associate so that the foundation or business associate may contact patients to raise money for the foundation. We will only use the following information without a patient's permission: contact information, such as a name, address and phone number; dates of treatment or services; the general department in which the patient was treated; the name of the treating physician; and, if the patient had less than an optimal outcome, that information as well. Note: Norton Healthcare does not require patients to participate in receiving fundraising communications in order to receive treatment. Patients who do not want to be contacted for fundraising efforts must notify the Foundations Office in writing at 234 E. Gray St., Suite 450, Louisville, KY 40202.

Marketing activities. We may, without obtaining authorization and so long as we do not receive payment from a third party for doing so, (1) provide patients with marketing materials in a face-to-face encounter, (2) give patients a promotional gift of nominal value, and/or (3) tell patients about our own health care products and services. We will ask patients' permission to use their health information for any other marketing activities.

Hospital directory. Norton Healthcare may include certain limited information about patients in a directory while they are patients in the hospital. This information may include name, location in the hospital and general condition (e.g., fair, stable, etc.). The directory information, except for religious affiliation, may be released to people who ask for patients by name. Additionally, a patient's religious affiliation may be provided to a member of the clergy, such as a priest or rabbi, even if they do not ask for

a patient by name. This release of information is so a patient's family, friends and clergy can visit the patient in the hospital and generally know how he or she is doing. Patients may restrict whether their information is included in the directory by notifying patient access at the point of registration or their nurse at any time during their stay.

Individuals involved in care or payment for care. Norton Healthcare may release medical information about patients to a friend or family member who is involved in the patient's medical care or payment for the patient's care. We may use or disclose a patient's medical information to notify or assist in the notification of a patient's family or other persons responsible for patient care about the patient's location, general condition or death. In addition, we may disclose medical information about a patient to an entity assisting in disaster relief efforts so the patient's family can be notified about the patient's condition, status and location.

Research. Medical research is vital to the advancement of medical science. Federal regulations permit use of patient medical information in research, either with patient authorization or when the research study is reviewed and approved by an Institutional Review Board or privacy board before any medical research study begins. In some situations, limited information may be used before approval of the research study to allow a researcher to determine whether enough patients exist to make a study scientifically valid. Institutional Review Boards and privacy boards follow a special review process to protect patient safety, welfare and confidentiality. Norton Healthcare will use and disclose medical information about patients for research purposes only as permitted by federal and state law.

As required by law. Norton Healthcare will disclose medical information about patients when required to do so by federal, state or local law.

To avoid a serious threat to health or safety. Norton Healthcare may use and disclose medical information about patients when consistent with applicable law and ethical standards to prevent or lessen a serious and imminent threat to the health and safety of a person or the public. Any disclosure, however, would be only to someone able to lessen or prevent the threat.

Business associates. Norton Healthcare may contract with other entities, called business associates, for the provision of certain services that require the business associates to use and disclose medical information to perform a service on behalf of Norton Healthcare. Examples of business associates of Norton Healthcare include medical transcription providers and companies that assist with patient billing and collection activities. Norton Healthcare enters into "business associate agreements" with these types of entities. These agreements, as well as federal law, require business associates to protect patient medical information.

Participation in health information exchanges. We may participate in one or more health information exchanges (HIEs) and may electronically share your health information for treatment, payment and permitted healthcare operations purposes with other participants in the HIE, including entities that may not be listed under "Who will follow this notice." Patients may "opt out" of HIE participation by contacting the Norton Healthcare Health Information Management Department. HIEs allow patients' health care providers to efficiently access and use your pertinent medical information necessary for treatment and other lawful purposes. We will not share patients' information with an HIE unless we have entered into a business associate agreement with the HIE to protect the confidentiality of patients' information.

Participation in a shared electronic medical record. Norton Healthcare facilities may participate in a shared electronic medical record with other health care providers in the community. This makes it easier for a patient's health care providers to have access to the patient's health information, and it improves the quality of a patient's care. Patients who would like a list of the health care providers that participate in the shared medical record may contact the Norton Healthcare Health Information Management Department.

Special situations

Organ and tissue donation. If a patient is an organ donor, Norton Healthcare may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

Military. If a patient is a member of the armed forces, Norton Healthcare may release medical information about the patient as required by military command authorities. We also may release medical information about foreign military personnel to the appropriate foreign military authority.

Workers' compensation. Norton Healthcare may release medical information about patients for workers' compensation or similar programs that provide benefits for work-related injuries or illnesses.

Public health risks. Norton Healthcare may disclose medical information about patients for public health activities. Generally, these activities include the following reports:

- To prevent or control disease, injury or disability
- To report births and deaths
- To report to the appropriate government authority if Norton Healthcare suspects a patient has been the victim of abuse or neglect, including child abuse
- To report reactions to medications or problems with medical devices

- To notify people of recalls of products they may be using
- 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
- With a parent or guardian's verbal permission, to notify the school(s) attended by child(ren) concerning immunization

Health oversight activities. Norton Healthcare may disclose patients' medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, licensure or disciplinary actions and legal proceedings or actions. These activities are necessary for the government to monitor the health care system, government programs and compliance with civil rights laws.

Highly Confidential Information. Federal and state laws require special privacy protections for certain highly confidential information about patients ("Highly Confidential Information"), including the subset of protected health information that is maintained in psychotherapy notes or is about the patient's: (1) mental health and/or developmental disabilities services; (2) substance use disorder prevention, diagnosis, treatment or referral; (3) HIV/AIDS testing, diagnosis or treatment; (4) communicable disease(s); (5) genetic testing; (6) child abuse and neglect; (7) domestic or elder abuse; and/or (8) sexual assault. In order for the patient's Highly Confidential Information to be disclosed for a purpose other than those permitted by law, Norton Healthcare will require the patient's written authorization.

Lawsuits and disputes. Norton Healthcare may disclose medical information about the patient in response to a court order or administrative order. We also may disclose medical information about patients in response to a subpoena, discovery request or other lawful process.

Law enforcement. If asked to do so by law enforcement, and to the extent permitted or required by law, we may release medical information for the following reasons:

- In response to a court order, subpoena, warrant, summons or similar process
- To identify or locate a suspect, fugitive, material witness or missing person
- About a suspected victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement
- About a death suspected to be the result of criminal conduct
- About criminal conduct at any Norton Healthcare facility
- 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
- In an investigation of a patient's alleged unlawful attempt to obtain a controlled substance at a Norton Healthcare facility

Coroners, medical examiners and funeral directors. Norton Healthcare may release patients' medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We also may release medical information about patients to funeral directors as necessary to carry out their duties.

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

Protective services for the president and others. Norton Healthcare may disclose medical information about patients to authorized federal officials so they may provide protection to the president, other authorized persons or foreign heads of state or to conduct special investigations.

Inmates. If a patient is an inmate of a correctional institution, Norton Healthcare may release medical information about the patient to the correctional institution or to a law enforcement official who has custody. This release would be necessary: (l) for the institution to provide the patient with health care; (2) to protect the patient's health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

Patient rights regarding their personal medical information. Patients have the following rights regarding medical information Norton Healthcare maintains about them:

Right to inspect and copy. Patients have the right to inspect and copy medical information that may be used to make decisions about their care. Usually, this includes medical and billing records but does not include psychotherapy notes.

To inspect and copy medical or billing information, patients must submit their request in writing to the Norton Healthcare Health Information Management Department. If the facility uses or maintains an electronic health record with respect to medical information, patients have the right to obtain an electronic copy of the information if they so choose. If a patient requests an electronic copy of his or her information, we will provide the information in the format requested if it is feasible to do so. Patients may be charged a reasonable, cost-based fee for the costs of copying, mailing or other supplies associated with the request (for example, the costs may include the cost of a flash drive, if that is how the patient requested a copy of the information be produced).

A patient's request to inspect and copy personal medical information may be denied in certain circumstances. If access to medical information is denied, a patient may request that the denial be reviewed. Another licensed health care professional chosen by the facility will review the

request and the denial. The person conducting the review will not be the person who denied the request. Norton Healthcare will comply with the outcome of the review.

Right to amend. If a patient feels that medical information is incorrect or incomplete, the patient may ask that the information be amended. A patient has the right to request an amendment for as long as the information is kept by or for the facility.

Requests for amendments must be made in writing and submitted to the Norton Healthcare Health Information Management Department. In addition, the patient must provide a reason that supports the request.

Request for an amendment will be denied if it is not in writing or does not include a reason to support the request. In addition, requests also may be denied if the information:

- Was not created by Norton Healthcare, unless the patient provides a reasonable basis to believe the person or entity that created the information is no longer available to make the amendment
- Is not part of the medical information kept by or for the facility
- Is not part of the information that patients would be permitted to inspect or copy
- Is accurate and complete

Right to an accounting of disclosures. Patients have the right to request an "accounting of disclosures." This is a list of the disclosures Norton Healthcare made of medical information about the patient, except for disclosures: for treatment, payment and health care operations; that are incidental in nature; for our directory or to persons involved in care; for national security or intelligence purposes; to corrections institutions or law enforcement officials; or for disclosures made before April 14, 2003. For research disclosures, see the "Research" section in this notice.

To request this list, or accounting of disclosures, patients must submit a request in writing to the Norton Healthcare Health Information Management Department. Inpatients must give the written request to their nurse. Requests must state a time period that may not be longer than six years. Requests should indicate in what form the patient wants the list (for example, on paper or electronic). The first list requested within a 12-month period will be provided free. For additional lists during that same period, patients may be charged the cost of providing the list. Patients will be notified of the cost involved and may choose to withdraw or modify the request before any costs are incurred.

Right to request restrictions. Patients have the right to request a restriction on the medical information used or disclosed about them for treatment, payment or health care operations. Patients also have the right to request a limit on the medical information Norton Healthcare

discloses to someone who is involved in the patient's care or the payment for care, like a family member or friend, or for other permitted purposes. For example, patients could ask that we not use or disclose information about a surgery they had.

In most cases, Norton Healthcare is not required to agree to patient requests to restrict the use or disclosure of a patient's medical information. If a patient has paid out-of-pocket in full for items or services, the patient may request that information regarding the items or services not be disclosed to his/her health plan, and Norton Healthcare must grant such a request. In all other cases, Norton Healthcare is not required to agree to requests. If we do agree, we will comply with a patient's request unless the information is needed to provide emergency treatment and/or safe patient care.

To request restrictions, patients must make their request in writing to the Norton Healthcare Health Information Management Department. In the request, the patient must tell us: (I) what information he or she wants to limit; (2) whether he or she wants to limit our use, disclosure or both; and (3) to whom he or she wants the limits to apply (for example, disclosures to his or her spouse).

Right to request confidential communications. Patients have the right to ask that Norton Healthcare communicate with them about medical matters in a certain way or at a certain location. For example, a patient can ask that we contact him or her only at work or by mail.

To request confidential communications, patients must make their requests in writing to the Norton Healthcare Health Information Management Department. We will not ask the reason for the request. We will make every effort to accommodate all reasonable requests. Requests must specify how or where the patient wishes to be contacted and how payment will be handled.

Right to a paper copy of this notice. Patients have the right to a paper copy of this notice. Patients may ask us to provide a copy of this notice at any time. Even if a patient has agreed to receive this notice electronically, he or she is entitled to a paper copy of this notice.

Patients may obtain an electronic copy of this notice online at **NortonHealthcare.com**.

Right to be notified following a breach of the patient's unsecured protected health information. In the event that a patient's unsecured protected health information is compromised, Norton Healthcare will notify the patient of such an incident.

Changes to this notice

Norton Healthcare reserves the right to change this notice and to make the revised or changed notice effective for medical information we already have about patients as well as any

information we receive in the future. A copy of the current notice is posted in all our facilities. The notice contains the effective date on the cover page.

Complaints

If patients believe their privacy rights have been violated, they may file a complaint with the facility and/or with the secretary of the Department of Health and Human Services. Additionally, some states may allow the patient to file a complaint with the state's attorney general, Office of Consumer Affairs or other state agency as specified by applicable state law. To file a complaint with a Norton Healthcare facility, patients should contact the Norton Healthcare Health Information Management Department or the Compliance Hotline **(866) 264-4567**. All complaints must be submitted in writing. No one will be penalized or retaliated against for filing a complaint.

Other uses of medical information

Other uses and disclosures of medical information not covered by this notice or the laws that apply to Norton Healthcare will be made only with the patient's written permission or as otherwise permitted by law. If a patient provides us with permission to use or disclose medical information about them, they may revoke that permission, in writing, at any time. If a patient revokes permission, we will no longer use or disclose medical information about them for the reasons covered by their written authorization. We are unable to take back any disclosures we have already made with the patient's permission, and we are required to retain our records of the patient care that we provide.

Norton Healthcare complies with applicable federal civil rights laws and does not discriminate on the basis of race, color, national origin, age, disability, or sex.

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al **(866) 862-2636**

注意：如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 **(866) 862-2636**

Norton Healthcare

For more than 130 years, Norton Healthcare's faith heritage has guided its mission to provide quality health care to all those it serves. Today, Norton Healthcare is a leader in serving adult and pediatric patients from throughout Greater Louisville, Southern Indiana, the commonwealth of Kentucky and beyond.

About

Careers at Norton Healthcare
Get Healthy
About Norton Healthcare
Norton Healthcare Foundation
Quality Report
Refer a Patient
N-Store

Connect

Donate
For the media
Healthcare professionals
Employee resources
Contact

Get Healthy Newsletter

Enter your information below to sign up for our free Get Healthy e-mail newsletter. Once a week, you'll receive stories and insights from the Norton Healthcare family, right in your e-mail inbox.

Enter your e-mail

Español Privacy Policy HIPAA Disclaimer

200 E. Chestnut St. Louisville, KY 40202 • (502) 629-1234

EXHIBIT B

Although our review is ongoing, an initial analysis confirms Norton Healthcare was the victim of a cyber-event. Our Information Services team and cybersecurity experts are working to thoroughly inspect and determine the scope of the event. We have notified law enforcement.

More information

Norton Healthcare Network Update

Story by: Norton Healthcare on May 11, 2023

Updated Thursday, May 11, 5:50 p.m.

Although our review is ongoing, an initial analysis confirms Norton Healthcare was the victim of a cyber-event. Our Information Services team and cybersecurity experts are working to thoroughly inspect and determine the scope of the event. We have notified law enforcement.

As we learn more details of the impact of the event, we will be transparent with employees and the community about next steps.

This event began on Tuesday, when the security team received a suspicious communication related to information systems. In response, systems were immediately taken offline and internet and email access were disabled as a precaution to further protect the network. Teams are working to restore normal computer operations as quickly and safely as possible.

Hospitals, other facilities and medical practices remain open while caregivers follow protocols for times in which systems are down. Patients should continue to arrive for appointments at regular times unless otherwise contacted by phone.

Filed 23-CI-003349 11/21/2023 David L. Nicholson, Jefferson Circuit Clerk

Health care systems around the country have dealt with similar cyber events and cybersecurity is a top concern for Norton Healthcare. Our commitm
not changed.

Although our review is ongoing, an initial analysis confirms Norton Healthcare was the victim of a cyber-event. Our Information Services team and cybersecurity experts are working to thoroughly inspect and determine the scope of the event. We have notified law enforcement.

More information

Norton Healthcare

For more than 130 years, Norton Healthcare's faith heritag
to all those it serves. Today, Norton Healthcare is a leader
throughout Greater Louisville, Southern Indiana, the comm

About

Careers at Norton Healthcare
Get Healthy
About Norton Healthcare
Norton Healthcare Foundation
Quality Report
Refer a Patient
N-Store

Connect

Donate
For the media
Healthcare professionals
Employee resources
Contact

Get Healthy Newsletter

Enter your information below to sign up for our free Get Healthy e-mail newsletter. Once a week, you'll receive stories and insights from the Norton Healthcare family, right in your e-mail inbox.

Enter your e-mail

Español Privacy Policy HIPAA Disclaimer

200 E. Chestnut St. Louisville, KY 40202 • (502) 629-1234

EXHIBIT C

Recently, Norton Healthcare was the victim of a cyber-event. Unfortunately, this is causing long wait times for those trying to reach us by phone, as well as delays in network-related capabilities.

Here's what we can tell you

Norton Healthcare Network Update

Story by: Norton Healthcare on May 19, 2023

Updated Monday, May 22, 8:30 p.m.

Recently, Norton Healthcare was the victim of a cyber event. Unfortunately, this is causing long wait times for those trying to reach us by phone, as well as delays in network-related capabilities. This includes imaging, lab/test results, prescription fulfillment and Norton MyChart messaging. Please note that our providers are working through a backlog of MyChart messages, and the normal response time is 3 to 5 business days.

If you are seeking a prescription refill, all uncontrolled medications are still being called into the pharmacy of the patient's choosing.

If you are awaiting test or imaging results, we are working as quickly as we can to bring systems back online. Patients with urgent medical needs will be attended to first.

If you are concerned about a scheduled procedure, your provider's office will call you directly to notify you of any potential changes in your upcoming care.

If you are seeking a same-day appointment for an illness or minor injury and do not need emergency care, please visit one of our urgent care locations: Norton Prompt Care clinics and

Norton Immediate Care Centers.

Thank you for your patience and understanding.

Previous Update Friday, May 19, 11:15 a.m.

This has been a challenging time for our organizat
show compassion to our community. We always p

What took place on May 9 is a part of an active, th
what we can tell you.

Recently, Norton Healthcare was the victim of a cyber-event. Unfortunately, this is causing long wait times for those trying to reach us by phone, as well as delays in network-related capabilities.

Here's what we can tell you

We want to let the community know what is being done to address this issue. Caregivers follow established procedures when systems are offline. They may have to utilize manual processes and paper, but they are working hard to ensure patients receive the care they need.

We understand the community has many questions. We know our patients have questions. We do too and experts are working as quickly as they can to get answers. Here's what we can tell you:

On Tuesday, May 9, our Information Services team members noticed suspicious activity on our network and also were alerted to the receipt of a faxed communication containing threats and demands. As this matter is under investigation, we are unable to share specifics of the message.

While network systems were still operational, our cyber-security experts immediately and proactively took our network offline to further protect our systems. Then a thorough analysis of our network began.

Within days, we learned that Norton Healthcare was the victim of a cyber-event and we contacted the FBI.

Our CEO and entire leadership team have been dedicated to getting answers, restoring the network and working diligently to support our teams.

This investigation is ongoing and we are dedicating significant resources to get answers.

Cyber security experts recommend that you keep a close eye on your bank and investment accounts, as well as regularly change your account passwords. If you suspect any unusual activity on your account, notify your banking institution.

We are analyzing each application thoroughly to determine if there is a security risk to bring it back online. Everyone on these teams is working as quickly as they can. This is an incredibly time-consuming but critical process.

This was a cyber-event that happened to us. Sadly, [illegible] country to many businesses and healthcare syste[illegible]

Despite all the precautions we have taken and sign[illegible] we were still the victim of a crime.

Due to the tremendous efforts of our Information S[illegible] control. This bears repeating: At no point did an ex[illegible] network. All of our facilities remain open and patie[illegible]

Thank you for your patience and understanding. W[illegible] become available.

Recently, Norton Healthcare was the victim of a cyber-event. Unfortunately, this is causing long wait times for those trying to reach us by phone, as well as delays in network-related capabilities.

Here's what we can tell you

Norton Healthcare

For more than 130 years, Norton Healthcare's faith heritage has guided its mission to provide quality health care to all those it serves. Today, Norton Healthcare is a leader in serving adult and pediatric patients from throughout Greater Louisville, Southern Indiana, the commonwealth of Kentucky and beyond.

About

Careers at Norton Healthcare
Get Healthy
About Norton Healthcare
Norton Healthcare Foundation
Quality Report
Refer a Patient
N-Store

Connect

Donate
For the media
Healthcare professionals
Employee resources
Contact

Get Healthy Newsletter

Enter your information below to sign up for our free Get Healthy e-mail newsletter. Once a week, you'll receive stories and insights from the Norton Healthcare family, right in your e-mail inbox.

Enter your e-mail

Recently, Norton Healthcare was the victim of a cyber-event. Unfortunately, this is causing long wait times for those trying to reach us by phone, as well as delays in network-related capabilities.

Here's what we can tell you

200 E. Chestnut St. Louisville,

EXHIBIT D

May 24 Norton Healthcare Network Update

Story by: Norton Healthcare on May 24, 2023

Updated Wednesday, May 24, 6:30 p.m.

Thank you for choosing Norton Healthcare and Norton Children's for your care. We are here to serve the community and we want to keep you informed about the cyber event that happened to our network on May 9. The event remains under investigation. We continue to bring systems back online and are closer to resuming all operations. Below is updated information about our systems and what patients can expect while the review is underway.

Online Scheduling & e-Check-in

Online scheduling and e-Check-in are available through the Norton MyChart website and app. Norton eCare is also available. If you have questions, please call (502) 629-1234.

Billing Information

Billing information remains available within your Norton MyChart account. When we are able to accept online payments, patients will be notified.

Prescription Refills

If you are seeking a prescription refill, medications can be called into the pharmacy of the patient's choosing. If your prescription is not availa provider's office.

Test and Imaging Results

Our providers are working hard to communicate th that information with you as quickly as possible.

Scheduled Procedures

If you have questions about a scheduled procedure your provider's office directly or your provider will r

Same-Day and Urgent Care

If you are seeking a same-day appointment for an illness or minor injury and do not need emergency care, you can visit Norton Prompt Care clinics and Norton Immediate Care Centers.

You can reserve a spot online for Norton Immediate Care Centers at NortonHealthcare.com/ICC. For Norton Prompt Care clinics, please call (502) 446-5555.

Communications

Patients are encouraged to call the Norton Healthcare access center (502) 629-1234, or the Norton Children's access center (502) 629-KIDS (5437), with any questions they may have about care.

The answers to some of your questions may be available on NortonHealthcare.com or NortonChildrens.com. Providers are responding to voicemail messages as well as Norton MyChart messages as quickly as possible. We ask for patience as we are receiving more calls and messages.

Security of information

Norton Healthcare is working with third party specialists to carefully examine and safely restore all network applications following the cyber event. This process is a time consuming but critical part of the restoration process. We appreciate your patience as the investigation continues.

For more than 130 years, Norton Healthcare's faith heritage has guided its mission to provide quality health care to all those it serves. Today, Norton Healthcare is a leader throughout Greater Louisville, Southern Indiana, the comm

We are here to serve the community and we want to keep you informed about the cyber event that happened to our network on May 9. The event remains under investigation. We continue to bring systems back online and are closer to resuming all operations.

Read the latest

About

Careers at Norton Healthcare
Get Healthy
About Norton Healthcare
Norton Healthcare Foundation
Quality Report
Refer a Patient
N-Store

Get Healthy Newsletter

Enter your information below to sign up for our free Get Healthy e-mail newsletter. Once a week, you'll receive stories and insights from the Norton Healthcare family, right in your e-mail inbox.

Enter your e-mail

Español Privacy Policy HIPAA Disclaimer

200 E. Chestnut St. Louisville, KY 40202 • (502) 629-1234

Filed 23-CI-003349 11/21/2023 David L. Nicholson, Jefferson Circuit Clerk