IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

JOYCE TARVIS, individually and on behalf of all others similarly situated, Plaintiff, v. LIFESPAN PHYSICIAN GROUP OF MASSACHUSETTS, INC. d/b/a BROWN HEALTH MEDICAL GROUP-MA, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Joyce Tarvis ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Lifespan Physician Group of Massachusetts, Inc. d/b/a Brown Health Medical Group-MA ("Brown Health" or "Defendant"), and alleges as follows based upon personal knowledge as to her own acts and experiences, and, as to all other matters, upon information and belief, including the investigation of counsel:

I. NATURE OF THE ACTION

1. This is a class action arising out of a data breach that compromised the personal, financial, and protected health information of Plaintiff and hundreds of thousands of other patients of Brown Health, a multi-specialty, physician-led medical group that provides outpatient and ambulatory medical care in Massachusetts and the surrounding region (the "Data Breach").

2. Brown Health is part of the Brown University Health system (formerly Lifespan Corporation), the largest healthcare system in Rhode Island, which is headquartered at 167 Point Street, Providence, Rhode Island. To obtain care, patients like Plaintiff, including many residents

of Rhode Island, were required to entrust Brown Health with highly sensitive personal and medical information.[1]

3. On or about December 16, 2025, Brown Health became aware of a data security incident affecting a file server on its network. Brown Health has confirmed that an unauthorized actor gained access to that server between on or about December 15 and December 16, 2025. Upon information and belief, the files on that server contained the private information of Plaintiff and the proposed Class, and that information was accessed and may have been acquired by the unauthorized actor.[2]

4. According to Brown Health's own notice, the information maintained on the affected server and placed at risk in the Data Breach included patients' names, dates of birth, and contact information; health insurance information; billing, claims, and payment information; medical information; and, for at least some individuals, Social Security numbers, driver's license numbers or other government-issued identification numbers, credit or debit card numbers, and financial account information. Brown Health has stated that not all categories of information were affected for all individuals.

5. The scope of the compromise was substantial. Brown Health has reported that the Data Breach affected at least 290,357 residents of Massachusetts, along with residents of Rhode Island, Vermont, and other States.[3]

[1]See About Brown University Health, Brown University Health, https://www.brownhealth.org (last visited July 21, 2026).
[2]Notice of Data Breach, Lifespan Physician Group of Massachusetts, Inc. d/b/a Brown Health Medical Group-MA (dated July 16, 2026) ("Notice Letter") (on file with counsel).
[3]Commonwealth of Mass., Office of Consumer Affairs & Bus. Regulation, Data Breach Report 2026 (reporting 290,357 affected Massachusetts residents); Vt. Office of the Att'y Gen., Security Breach Notice (filed July 16, 2026) (reporting 86 affected Vermont residents).

6. The Data Breach was a direct and foreseeable result of Brown Health's failure to implement and maintain reasonable data-security measures appropriate to the sensitivity of the information it collected and stored, and consistent with well-established standards applicable to healthcare providers.

7. Plaintiff has already experienced concrete misuse of her information: after the Data Breach, and after Brown Health disclosed that the affected server contained payment-card and financial-account information that may have been affected, Plaintiff incurred fraudulent charges on her credit card that she did not authorize, and was required to cancel the card and obtain a replacement.

8. As a result of the Data Breach, Plaintiff and members of the proposed Class have suffered injury, including the compromise and misuse of their private information, an imminent and substantial risk of identity theft and fraud, the loss of the benefit of their bargain, the diminution in value of their private information, and the lost time and expense of responding to the breach.

9. Plaintiff brings this action to recover damages and to obtain injunctive and equitable relief requiring Brown Health to adopt reasonable security practices adequate to protect the information that remains in its possession.

10. The information Brown Health collects from its patients is precisely the kind of information that criminals prize: durable identifiers and health information that cannot be cancelled or reissued and that can be exploited for years after it is stolen. Brown Health knew, or should have known, that this information was a target and that its compromise would expose patients to a serious and lasting risk of harm.

11. The measures that would have prevented or mitigated the Data Breach were well established, widely published, and readily available. Federal and state regulators and recognized standard-setting bodies have for years prescribed the specific safeguards that a healthcare provider holding this information is expected to implement. Brown Health's failure to implement one or more of those safeguards exposed Plaintiff and the Class to a well-known and foreseeable risk.

12. Although Brown Health became aware of the incident on or about December 16, 2025, it did not notify affected individuals until on or about July 16, 2026, approximately seven months later. Brown Health has not publicly explained the reason for this seven-month interval between discovery and notice, during which Plaintiff and the Class were deprived of the opportunity to protect themselves.

II. PARTIES

13. Plaintiff Joyce Tarvis is a natural person and, at all relevant times, a citizen and resident of Tiverton, Newport County, Rhode Island. Plaintiff is a patient of Brown Health and provided her private information to Brown Health in connection with receiving medical care.

14. Defendant Lifespan Physician Group of Massachusetts, Inc. does business as Brown Health Medical Group-MA. It is a non-profit corporation organized under the laws of the Commonwealth of Massachusetts on September 25, 2024, and it operates physician and clinical practices, including a location on Faunce Corner Road, Dartmouth, Massachusetts 02747.

15. Upon information and belief, and as reflected in Defendant's corporate filings, Defendant's officers and directors direct, control, and coordinate Defendant's activities from 167 Point Street, Providence, Rhode Island, which is also the headquarters of Defendant's parent, Brown University Health (formerly Lifespan Corporation). Defendant's principal place of

business and nerve center are therefore located in Rhode Island, and Defendant is a citizen of both Rhode Island and Massachusetts.

III. JURISDICTION AND VENUE

16. This Court has subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The proposed Class consists of at least 100 members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. The minimal diversity required by 28 U.S.C. § 1332(d)(2)(A) is satisfied because Defendant is a citizen of Rhode Island and Massachusetts, while the proposed Class includes at least 86 citizens of Vermont, as well as citizens of other States, each of whom is a citizen of a State different from Defendant. The proposed Class is nationwide and includes hundreds of thousands of individuals residing in Massachusetts, Rhode Island, Vermont, and other States.

17. This Court has personal jurisdiction over Brown Health because Brown Health's principal place of business and nerve center are located in Providence, Rhode Island, as reflected in Defendant's corporate filings, which identify its officers and directors as located at 167 Point Street, Providence, Rhode Island, such that it is at home in this District; because Brown Health purposefully directs its activities at Rhode Island, including by serving Rhode Island patients such as Plaintiff and by, upon information and belief, directing its data-governance and information-security functions from Rhode Island; and because the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b) because Brown Health resides in this District and because a substantial part of the events or omissions giving rise to Plaintiff's claims, including Brown Health's decisions concerning the security of the information entrusted to it, occurred in and emanated from this District.

IV. FACTUAL ALLEGATIONS

A. Brown Health collects and stores sensitive patient information.

19. Brown Health is a multi-specialty, physician-led medical group that has provided outpatient and ambulatory medical care in Massachusetts and the surrounding region as part of the Brown University Health system.[4]

20. Brown Health offers a broad range of medical services, including primary care, pediatrics, behavioral health, women's health, dental, and pharmacy services, across numerous medical group locations.

21. In the ordinary course of providing these services, Brown Health requires its patients, including Plaintiff, to provide sensitive personal and medical information as a condition of receiving care.

22. Upon information and belief, the information Brown Health collects and maintains about its patients includes identifying information such as names, addresses, dates of birth, and contact information; health insurance information; billing, claims, and payment information; medical information; and, for at least some patients, Social Security numbers, driver's license numbers or other government-issued identification numbers, credit or debit card numbers, and financial account information (collectively, "private information").

23. Patients entrusted this information to Brown Health with the reasonable expectation that Brown Health would safeguard it and use it only for legitimate purposes, consistent with Brown Health's legal obligations and its own representations.

B. Brown Health represented that it would protect patient information.

[4]See About Brown University Health, Brown University Health, https://www.brownhealth.org (last visited July 21, 2026).

24. Brown Health solicited and required its patients to provide sensitive personal and health information as a condition of receiving care, and it did so against a backdrop of representations and obligations, express and implied, that it would keep that information confidential and secure.

25. Upon information and belief, Brown Health maintained a privacy policy or notice of privacy practices, as required of healthcare providers, in which it represented that it would protect the confidentiality of patient information and would use and disclose that information only for permitted purposes.

26. As a healthcare provider subject to the HIPAA Privacy and Security Rules, Brown Health was obligated to furnish patients with a notice of its privacy practices and to safeguard their protected health information. Patients reasonably relied on these representations and obligations in entrusting their information to Brown Health.

27. Plaintiff and the Class reasonably understood and expected that, in exchange for their information and their payment for services, Brown Health would provide reasonable data security. That expectation was a basic, if implicit, term of their relationship with Brown Health.

C. The Data Breach.

28. According to Brown Health, on or about December 16, 2025, it became aware of a data security incident impacting a file server on its network.[5]

29. Upon information and belief, an unauthorized actor gained access to that server between on or about December 15 and December 16, 2025, and files containing the private

[5]Notice of Data Breach, Lifespan Physician Group of Massachusetts, Inc. d/b/a Brown Health Medical Group-MA (dated July 16, 2026) ("Notice Letter") (on file with counsel).

information of Plaintiff and members of the proposed Class were accessed and may have been acquired.[6]

30. Brown Health has represented that the incident did not affect its electronic health record system. The affected file server nonetheless contained extensive and highly sensitive private information, including demographic, insurance, billing, medical, and financial data and, for at least some individuals, Social Security numbers, government-issued identification numbers, and payment-card and financial-account information. Brown Health has further stated that it was unable to conclusively determine exactly what information was affected, that it determined the scope of the potentially affected information on or about June 22, 2026, and that not all categories of information were affected for all individuals.[7]

31. Because an unauthorized actor gained access to files containing this sensitive information, the private information of Plaintiff and the Class is at continuing risk of misuse. Brown Health has stated that it isolated the affected server, notified law enforcement, and offered affected individuals twenty-four months of complimentary Experian IdentityWorks credit-monitoring and identity-restoration services, an acknowledgment of the risk of identity theft and fraud created by the Data Breach.

D. Brown Health's data-security obligations.

32. As a healthcare provider entrusted with protected health information, and as an entity holding the personal information of residents of Rhode Island and Massachusetts, Brown Health was subject to well-established legal and industry obligations to safeguard the information in its custody.

[6]Notice Letter, supra.
[7]Notice Letter, supra.

33. The Health Insurance Portability and Accountability Act ("HIPAA") and its implementing Security Rule establish a recognized standard of care for the protection of electronic protected health information, requiring covered entities to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of such information. See 45 C.F.R. §§ 164.302–164.318. *HIPAA is pleaded here solely as a reference for the applicable standard of care and not as an independent cause of action or as a basis for negligence per se.*

34. The U.S. Department of Health and Human Services has long published guidance confirming that reasonable cybersecurity safeguards are a settled expectation for healthcare organizations, not a novel obligation.[8]

35. Federal guidance specific to the healthcare sector identifies foundational safeguards that providers are expected to implement, including email protection, endpoint protection, access management, data protection, vulnerability management, and incident-response planning.[9] The Department has further identified sector cybersecurity performance goals prioritizing multifactor authentication, encryption, credential management, and incident planning.[10]

36. Beyond the healthcare sector, the Federal Trade Commission has repeatedly instructed businesses that reasonable data security requires inventorying stored personal information, securely disposing of data that is no longer needed, encrypting sensitive information, understanding system vulnerabilities, and planning for breaches.[11] The FTC has likewise

[8]U.S. Dep't of Health & Human Servs., Off. for Civil Rights, Security Rule Guidance Material, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited July 7, 2026).
[9]U.S. Dep't of Health & Human Servs., 405(d) Program, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (2023 ed.), https://405d.hhs.gov/Documents/HICP-Main-508.pdf (last visited July 7, 2026).
[10]U.S. Dep't of Health & Human Servs., Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (2024), https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf (last visited July 7, 2026).
[11]Fed. Trade Comm'n, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited July 7, 2026).

emphasized building security into operations from the outset, including access controls, strong authentication, network segmentation and monitoring, and timely patching.[12]

37. Widely recognized technical frameworks define the baseline of reasonable security. The National Institute of Standards and Technology publishes a comprehensive catalog of security and privacy controls addressing access control, authentication, audit and logging, incident response, and risk assessment.[13] The Center for Internet Security publishes a prioritized set of Critical Security Controls that represents industry consensus on reasonable security practices.[14]

38. Brown Health failed to implement one or more of these basic, well-established safeguards, and, upon information and belief, one or more of those failures permitted or materially contributed to the unauthorized access to the private information of Plaintiff and the Class.

E. Reasonable security required specific, well-defined safeguards that Brown Health failed to implement.

39. The measures that constitute reasonable data security for an organization holding sensitive personal and health information are not vague aspirations; they are specific, cataloged, and freely published. The National Institute of Standards and Technology maintains a comprehensive control catalog addressing, among other families, access control, identification and authentication, audit and accountability, incident response, risk assessment, and system and information integrity.[15]

---

[12]Fed. Trade Comm'n, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited July 7, 2026).

[13]Joint Task Force, Nat'l Inst. of Standards & Tech., Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Rev. 5 (Sept. 2020), https://doi.org/10.6028/NIST.SP.800-53r5 (last visited July 7, 2026).

[14]Ctr. for Internet Sec., CIS Critical Security Controls (v8.1) (2024/2025), https://www.cisecurity.org/controls/v8-1 (last visited July 7, 2026).

[15]Joint Task Force, Nat'l Inst. of Standards & Tech., Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Rev. 5 (Sept. 2020), https://doi.org/10.6028/NIST.SP.800-53r5 (last visited July 7, 2026).

40. The Center for Internet Security publishes a prioritized set of Critical Security Controls, including inventory and control of assets, continuous vulnerability management, controlled use of administrative privileges, maintenance and monitoring of audit logs, malware defenses, boundary defense, and data protection, that represents industry consensus on the safeguards a reasonable organization must implement.[16]

41. For healthcare organizations specifically, the Department of Health and Human Services, through its 405(d) program, identified a set of practical safeguards keyed to the sector's most significant threats, including email protection, endpoint protection, access management, data protection and loss prevention, and vulnerability management.[17] The Department separately articulated sector cybersecurity performance goals emphasizing multifactor authentication, encryption, credential management, and incident planning as foundational.[18]

42. The Federal Trade Commission has distilled comparable expectations from decades of enforcement, instructing businesses to build security into their operations from the start, to control access to data, to require secure authentication, to segment and monitor networks, to apply sound security practices when developing and maintaining systems, and to keep security current through patching and monitoring.[19] These expectations reflect a settled regulatory understanding of reasonable security, not a novel or shifting standard.[20]

---

[16]Ctr. for Internet Sec., CIS Critical Security Controls (v8.1) (2024/2025), https://www.cisecurity.org/controls/v8-1 (last visited July 7, 2026).

[17]U.S. Dep't of Health & Human Servs., 405(d) Program, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (2023 ed.), https://405d.hhs.gov/Documents/HICP-Main-508.pdf (last visited July 7, 2026).

[18]U.S. Dep't of Health & Human Servs., Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (2024), https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf (last visited July 7, 2026).

[19]Fed. Trade Comm'n, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited July 7, 2026).

[20]Fed. Trade Comm'n, Data Security (resource page), https://www.ftc.gov/business-guidance/privacy-security/data-security (last visited July 7, 2026).

43. Upon information and belief, Brown Health failed to implement one or more of these well-established safeguards, including, among others, adequate access controls and authentication, network monitoring and intrusion detection, timely patching and vulnerability management, encryption of sensitive data at rest, and workforce training, and that failure was a direct and proximate cause of the Data Breach.

F. The HIPAA Security Rule reflects the applicable standard of care.

44. As a healthcare provider, Brown Health was subject to the HIPAA Security Rule, which establishes a nationally recognized framework for safeguarding electronic protected health information. Plaintiff references the Security Rule solely as evidence of the applicable standard of care, not as an independent cause of action and not as a basis for negligence per se.

45. The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of the electronic protected health information they create, receive, maintain, or transmit; to protect against reasonably anticipated threats or hazards to the security of that information; to protect against reasonably anticipated impermissible uses or disclosures; and to ensure workforce compliance. See 45 C.F.R. § 164.306(a).

46. The Security Rule further requires covered entities to implement administrative, physical, and technical safeguards, including access controls that limit information-system access to authorized persons and software, audit controls, integrity controls, and transmission security. See 45 C.F.R. §§ 164.308, 164.310, 164.312.

47. The Department of Health and Human Services has long published guidance elaborating on these obligations and confirming that basic safeguards and cyber-preparedness are longstanding expectations for entities holding protected health information.[21]

[21] U.S. Dep't of Health & Human Servs., Off. for Civil Rights, Security Rule Guidance Material, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited July 7, 2026).

48. Brown Health's failure to prevent the unauthorized access to protected health information supports the inference that Brown Health did not meet the standard of care that the Security Rule reflects.

G. The Data Breach was foreseeable and preventable.

49. The risk that healthcare providers would be targeted by cyberattacks and data-theft campaigns was well known long before June 2026. Federal authorities have repeatedly warned that cyberattacks are a pervasive and evolving threat and have published detailed, freely available guidance on how to prevent and mitigate it.[22]

50. The exploitation of known, unpatched vulnerabilities is a leading vector for such attacks, and timely vulnerability management is a baseline cybersecurity function that federal authorities have long urged organizations to perform.[23]

51. Data breaches affecting the healthcare sector have become routine and are among the most common categories of reported data compromises, a trend documented in annual reporting on breach volume.[24]

52. Federal healthcare regulators have specifically recognized that cyberattacks present a foreseeable threat to protected health information and that a security incident triggers a covered entity's breach-analysis obligations.[25]

---

[22]Cybersecurity & Infrastructure Sec. Agency & Multi-State Info. Sharing & Analysis Ctr., #StopRansomware Guide (initial release Sept. 2020; updated Mar. 2025), https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf (last visited July 7, 2026).

[23]Cybersecurity & Infrastructure Sec. Agency, Known Exploited Vulnerabilities Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog (continuously updated) (last visited July 7, 2026).

[24]Identity Theft Res. Ctr., 2025 Data Breach Report (Twentieth Edition) (Jan. 2026), https://www.idtheftcenter.org/wp-content/uploads/2026/01/2025-ITRC-Annual-Data-Breach-Report.pdf (last visited July 7, 2026).

[25]U.S. Dep't of Health & Human Servs., Off. for Civil Rights, Fact Sheet: Ransomware and HIPAA (Sept. 20, 2021), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html (last visited July 7, 2026).

53. Given the sensitivity and volume of the information Brown Health collected, and the well-publicized wave of cyberattacks against healthcare providers, the Data Breach was a foreseeable consequence of Brown Health's failure to maintain reasonable security. Had Brown Health implemented the safeguards described above, the Data Breach could have been prevented or its impact materially limited.

H. Cyberattacks and data theft targeting healthcare providers were a known and escalating threat.

54. For years preceding the Data Breach, federal cybersecurity authorities repeatedly and publicly warned that healthcare providers were among the most heavily targeted victims of cyberattacks and data theft campaigns. The Cybersecurity and Infrastructure Security Agency, together with partner agencies, has published and repeatedly updated detailed guidance identifying cyberattacks as a pervasive threat and prescribing specific, freely available defensive controls.[26]

55. These warnings were not abstract. Federal healthcare regulators specifically advised covered entities that cyberattacks against protected health information were foreseeable, that such attacks trigger breach-analysis obligations, and that entities must prepare contingency and response plans in advance.[27]

56. Upon information and belief, Defendant's corporate family had prior notice of the need for robust safeguards for protected health information. In 2020, an affiliated covered entity within the Lifespan (now Brown University Health) system, of which Defendant is a part, paid $1,040,000 to the U.S. Department of Health and Human Services' Office for Civil Rights to resolve findings that it had failed to encrypt and adequately safeguard protected health information

[26]Cybersecurity & Infrastructure Sec. Agency & Multi-State Info. Sharing & Analysis Ctr., #StopRansomware Guide (initial release Sept. 2020; updated Mar. 2025), https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf (last visited July 7, 2026).

[27]U.S. Dep't of Health & Human Servs., Off. for Civil Rights, Fact Sheet: Ransomware and HIPAA (Sept. 20, 2021), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html (last visited July 7, 2026).

following the theft of an unencrypted laptop. That resolution put Defendant's corporate family on notice of its obligation to encrypt and safeguard protected health information.[28]

57. The scale of healthcare-sector breaches underscored the risk. Annual reporting on data-compromise volume has repeatedly identified healthcare as one of the most-affected sectors, with the number of reported compromises and affected individuals reaching record levels in recent years.[29]

58. Numerous large, well-publicized cyberattacks and data-theft incidents affecting healthcare organizations preceded the Data Breach and placed the entire sector, including Brown Health, on notice that providers holding protected health information were prime targets and that reasonable, current safeguards were essential.[30]

59. Brown Health, as a healthcare provider subject to federal and state health-privacy and data-security obligations, knew or should have known of these warnings and of the acute risk to the sensitive information in its custody. The foreseeability of exactly this kind of attack heightened Brown Health's duty to implement robust, current safeguards.[31]

60. The methods by which threat actors gain access to victim networks are well documented and defensible against. Attackers routinely exploit known, publicly cataloged software vulnerabilities for which patches are available, compromise credentials through phishing, and move laterally through networks that lack segmentation and monitoring. Federal authorities

---

[28] See Press Release, U.S. Dep't of Health & Human Servs., Off. for Civil Rights, Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach (July 27, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lifespan/index.html (last visited July 21, 2026).

[29] Identity Theft Res. Ctr., 2025 Data Breach Report (Twentieth Edition) (Jan. 2026), https://www.idtheftcenter.org/wp-content/uploads/2026/01/2025-ITRC-Annual-Data-Breach-Report.pdf (last visited July 7, 2026).

[30] Identity Theft Res. Ctr., 2025 Data Breach Report (Twentieth Edition) (Jan. 2026), https://www.idtheftcenter.org/wp-content/uploads/2026/01/2025-ITRC-Annual-Data-Breach-Report.pdf (last visited July 7, 2026).

[31] U.S. Dep't of Health & Human Servs., Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (2024), https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf (last visited July 7, 2026).

maintain and continuously update a public catalog of known exploited vulnerabilities precisely so that organizations can prioritize remediation and close these avenues of attack.[32]

61. Because these attack methods are known and the corresponding defenses are established, a successful intrusion of the kind alleged here is consistent with a failure to implement one or more baseline safeguards, such as timely patching, multifactor authentication, network segmentation, and continuous monitoring.[33]

62. Federal incident-response guidance further recognizes that organizations must prepare for security incidents in advance and integrate incident response into their overall risk-management program, so that when an incident occurs the organization can rapidly detect, contain, and remediate it and limit the harm to affected individuals.[34]

63. Brown Health's failure to prevent, detect, and contain the Data Breach, and the resulting unauthorized access to and potential exposure of the private information of Plaintiff and the Class, reflects a departure from these well-established expectations.

I. Brown Health's response obligations.

64. Upon discovering a cyberattack, a healthcare entity is expected to promptly identify and respond to the incident, mitigate harm, and provide affected individuals with timely and accurate notice of the nature and scope of the compromise.[35] Established incident-response

[32]Cybersecurity & Infrastructure Sec. Agency, Known Exploited Vulnerabilities Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog (continuously updated) (last visited July 7, 2026).
[33]Cybersecurity & Infrastructure Sec. Agency & Multi-State Info. Sharing & Analysis Ctr., #StopRansomware Guide (initial release Sept. 2020; updated Mar. 2025), https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf (last visited July 7, 2026).
[34]Nat'l Inst. of Standards & Tech., Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST Special Publication 800-61, Rev. 3 (Apr. 2025), https://csrc.nist.gov/pubs/sp/800/61/r3/final (last visited July 7, 2026).
[35]U.S. Dep't of Health & Human Servs., Off. for Civil Rights, My Entity Just Experienced a Cyber-Attack! What Do We Do Now? A Quick-Response Checklist (June 2017), https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf (last visited July 7, 2026).

guidance requires organizations to integrate incident handling into their broader risk-management program to reduce impact and speed detection, response, and recovery.[36]

65. The FTC's data-breach-response guidance similarly directs organizations to secure their systems, remediate vulnerabilities, preserve evidence, and provide required notifications without delay.[37]

66. Timely and accurate notice is essential because it enables affected individuals to take protective measures, such as monitoring accounts, placing fraud alerts and credit freezes, and scrutinizing medical and insurance records, before their information is misused.

67. Rhode Island and Massachusetts law reflect this expectation. Rhode Island's Identity Theft Protection Act of 2015 requires that notice of a breach be made in the most expedient time possible but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information necessary to provide notice. See R.I. Gen. Laws § 11-49.3-4. Massachusetts law likewise requires notice as soon as practicable and without unreasonable delay. See M.G.L. c. 93H, § 3. These laws also reflect Brown Health's obligation, under R.I. Gen. Laws § 11-49.3-2 and 201 CMR 17.00, to maintain reasonable data-security safeguards for the information of Rhode Island and Massachusetts residents.

68. Independent of any statute, the HIPAA Breach Notification Rule requires covered entities to notify affected individuals of a breach of unsecured protected health information without unreasonable delay and in no case later than sixty days following discovery. See 45 C.F.R. §§

[36]Nat'l Inst. of Standards & Tech., Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST Special Publication 800-61, Rev. 3 (Apr. 2025), https://csrc.nist.gov/pubs/sp/800/61/r3/final (last visited July 7, 2026).

[37]Fed. Trade Comm'n, Data Breach Response: A Guide for Business (Aug. 2023), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last visited July 7, 2026).

164.400–414. These provisions are referenced as benchmarks for the notice Brown Health owed, not as independent causes of action.

69. Prompt, complete notice was particularly important here because the sensitivity of the compromised information means that early detection and mitigation can materially reduce the risk of downstream identity theft and medical identity theft. Brown Health's roughly seven-month delay, becoming aware of the incident on or about December 16, 2025, but not notifying affected individuals until on or about July 16, 2026, compounded the harm to Plaintiff and the Class.

J. The value of the compromised information and the resulting risk of harm.

70. The private information compromised in the Data Breach is valuable to criminals precisely because it can be used to commit identity theft, financial fraud, and medical identity theft, and because, unlike a payment-card number, core identifiers such as Social Security numbers, dates of birth, and medical histories cannot readily be changed or cancelled.

71. The Social Security Administration has explained that a compromised Social Security number can be used to commit tax fraud, benefits fraud, employment fraud, and financial fraud, and that the harms may recur over time.[38]

72. The misuse of stolen information is frequently delayed. The U.S. Government Accountability Office has found that stolen data may remain dormant for a year or more before it is used, and that fraudulent use can continue for years thereafter, such that the full extent of harm from a breach often cannot be measured immediately.[39] Federal consumer-protection authorities

[38]Soc. Sec. Admin., Identity Theft and Your Social Security Number, SSA Pub. No. 05-10064 (2018).

[39]U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2026).

have likewise cautioned that the absence of immediate confirmed fraud does not negate the present risk that stolen information will be misused.[40]

73. Because of the sensitivity of the information involved, Plaintiff and members of the Class face a present, imminent, and substantial risk of identity theft and fraud, and must devote time and resources to monitoring their financial, medical, and insurance records to detect and mitigate misuse.

K. Protected health information is uniquely valuable and uniquely dangerous when stolen.

74. Protected health information is among the most valuable categories of data to criminals because it is rich, durable, and difficult to remediate. A single medical record may combine identifying information, insurance details, and clinical history, information that cannot be cancelled or reissued the way a payment card can.

75. Unlike a compromised payment-card number, which a consumer can cancel to cut off the risk of further misuse, core identifiers such as Social Security numbers, dates of birth, and medical histories are effectively immutable. Once stolen, they can be exploited for years, and the harm compounds over time.[41]

76. Stolen health information enables medical identity theft, in which a criminal uses another person's identity or insurance to obtain treatment, prescriptions, or services, corrupting the victim's medical and insurance records and creating risks to both finances and health that can be extraordinarily difficult to unwind.

[40] Ari Lazarus, Fed. Trade Comm'n, How Fast Will Identity Thieves Use Stolen Info? (May 24, 2017), https://consumer.ftc.gov/consumer-alerts/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited July 7, 2026).

[41] Soc. Sec. Admin., Identity Theft and Your Social Security Number, SSA Pub. No. 05-10064 (2018).

77. The misuse of stolen data is frequently delayed, which makes the risk more dangerous, not less. The Government Accountability Office has found that stolen information may lie dormant for a year or more before it is used and that resulting harm can continue for years thereafter, such that the full extent of harm from a breach often cannot be measured at the outset.[42] Federal consumer-protection authorities have similarly cautioned that the absence of immediate confirmed misuse does not negate present risk.[43]

78. Because the information compromised in the Data Breach includes durable, sensitive identifiers and health information, Plaintiff and the Class face a present and continuing risk of identity theft, financial fraud, and medical identity theft that will persist for years and that requires ongoing vigilance to detect and mitigate.

L. Plaintiff and the Class must expend time and resources to mitigate the risk of harm.

79. When sensitive information is compromised, a reasonable person must take protective steps to guard against identity theft and fraud. Federal authorities recommend that breach victims review account statements and credit reports, place fraud alerts or credit freezes, monitor for unauthorized activity, and, for health information, scrutinize medical and insurance records for signs of misuse.[44]

[42] U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2026).

[43] Ari Lazarus, Fed. Trade Comm'n, How Fast Will Identity Thieves Use Stolen Info? (May 24, 2017), https://consumer.ftc.gov/consumer-alerts/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited July 7, 2026).

[44] U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2026).

80. These steps take time and, in many cases, money. The Government Accountability Office has recognized that victims of identity theft can face substantial costs and lost time to repair the damage to their credit and their records.[45]

81. Plaintiff and the Class have already been required, and will continue to be required, to devote time and resources to these protective measures as a direct and proximate result of the Data Breach, time and resources they would not otherwise have had to spend.

M. Plaintiff and the Class lost the benefit of their bargain and the value of their information.

82. A portion of the value that Plaintiff and the Class conferred on Brown Health, whether through direct payment, insurance, or public funding tied to their care, was reasonably understood to fund the reasonable data security that a healthcare provider is expected to maintain. Brown Health did not deliver that security.

83. Plaintiff and the Class therefore did not receive the full benefit of their bargain. Had they known that Brown Health would not maintain reasonable safeguards for their sensitive information, they would have paid less for Brown Health's services, taken additional protective measures, or declined to provide certain information.

84. Separately, personal and health information has recognized economic value, and a market exists in which such information is bought and sold, both lawfully and unlawfully. The compromise of that information in the Data Breach diminished its value to Plaintiff and the Class by stripping it of its confidentiality and exposing it to unauthorized use.

[45]U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2026).

85. The transfer and exposure of this information occurred without any compensation to Plaintiff or the Class, and the resulting loss of confidentiality and control constitutes a concrete economic injury independent of any subsequent fraud.[46]

N. The private information of Plaintiff and the Class remains at risk.

86. Upon information and belief, Brown Health continues to maintain the private information of Plaintiff and the Class in its systems, and Brown Health has not demonstrated that it has remediated the deficiencies that permitted the Data Breach or adopted safeguards sufficient to prevent a recurrence.

87. The continuing risk is heightened because the same categories of information that were compromised remain in Brown Health's custody and, upon information and belief, Brown Health has not demonstrated that it has remediated the vulnerabilities that permitted the Data Breach or adopted the safeguards necessary to prevent a recurrence.[47]

88. Injunctive and equitable relief is therefore necessary and appropriate. Federal guidance identifies the specific measures that a healthcare organization is expected to maintain, including multifactor authentication, encryption, access and credential management, vulnerability management, monitoring, and incident-response planning, and Brown Health should be required to implement and maintain such measures to protect the information that remains in its possession.[48]

---

[46]U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2026).

[47]U.S. Dep't of Health & Human Servs., 405(d) Program, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (2023 ed.), https://405d.hhs.gov/Documents/HICP-Main-508.pdf (last visited July 7, 2026).

[48]U.S. Dep't of Health & Human Servs., Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (2024), https://hhscyber.hhs.gov/documents/cybersecurity-performance-goals.pdf (last visited July 7, 2026).

89. So long as Brown Health retains this information without adopting reasonable safeguards, Plaintiff and the Class face a continuing risk of further unauthorized access and disclosure. Injunctive and equitable relief is necessary to address that ongoing risk.[49]

90. Because the private information of Plaintiff and the Class was accessed by an unauthorized actor, it remains at risk of misuse, sale, or disclosure well into the future.[50]

V. PLAINTIFF-SPECIFIC ALLEGATIONS

91. Plaintiff Joyce Tarvis is a patient of Brown Health. As a condition of receiving care, Plaintiff provided Brown Health with her sensitive personal and medical information.

92. Plaintiff reasonably expected and understood that Brown Health would maintain her information securely and would use it only for legitimate healthcare purposes. Plaintiff would not have provided her information, or would have taken additional protective measures, had she known that Brown Health's data-security practices were inadequate.

93. At the time of the Data Breach, Brown Health maintained Plaintiff's private information in its systems.

94. On or about July 20, 2026, Plaintiff received Brown Health's written Notice of Data Breach, which informed her that her private information was involved in the Data Breach and identified the categories of information that may have been affected in the incident, including Social Security numbers, financial account information, payment-card information, government-issued identification numbers, and medical information. The notice stated that not all categories of information were affected for all individuals. Plaintiff retains a copy of the notice letter.

---

[49] Nat'l Inst. of Standards & Tech., Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST Special Publication 800-61, Rev. 3 (Apr. 2025), https://csrc.nist.gov/pubs/sp/800/61/r3/final (last visited July 7, 2026).

[50] U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2026).

95. After the Data Breach, Plaintiff experienced fraudulent charges on her credit card that she did not authorize, in an approximate amount of $176, and was required to cancel the card and obtain a replacement. Plaintiff had not experienced such fraudulent charges before the Data Breach. The timing and nature of these charges were temporally and categorically consistent with the Data Breach, and, upon information and belief, the charges were caused or facilitated by the unauthorized access to payment-card and financial-account information maintained by Brown Health.

96. Since the Data Breach, Plaintiff has also experienced an increase in unsolicited spam email consistent with the exposure of her contact information. Plaintiff has enrolled in credit-monitoring services and has expended time responding to the Data Breach and the fraudulent charges on her account, and she remains at heightened risk of further identity theft and fraud.

97. As a direct and proximate result of the Data Breach, Plaintiff has suffered concrete and particularized injury, including: (i) the fraudulent charges incurred on her payment card as described above; (ii) the compromise and unauthorized exposure of her private information; (iii) a present, imminent, and substantial risk of further identity theft and fraud; (iv) the loss of time and effort reasonably incurred in responding to the Data Breach and the fraudulent charges; (v) the diminution in value of her private information; (vi) the loss of the benefit of the bargain; and (vii) the continued risk to her information that remains in Brown Health's possession.

VI. INJURIES COMMON TO THE CLASS

98. The Data Breach exposed Plaintiff and every member of the Class to the same categories of injury arising from the same course of conduct: Brown Health's failure to secure the private information entrusted to it.

99. Plaintiff and the Class have suffered, and will continue to suffer, injury including: (i) the compromise and unauthorized exposure of their private information; (ii) a present, imminent, and substantial risk of identity theft and fraud; (iii) the loss of time and out-of-pocket costs reasonably incurred in monitoring accounts and records and otherwise responding to the Data Breach; (iv) the diminution in value of their private information; (v) the loss of the benefit of the bargain; and (vi) the continued risk to information that remains in Brown Health's possession so long as Brown Health fails to adopt adequate safeguards.

100. These injuries flow directly from Brown Health's common course of conduct and are common to Plaintiff and every member of the Class.

101. The risk of future harm to Plaintiff and the Class is neither speculative nor remote. The information involved in the Data Breach is precisely the information that criminals use to commit identity theft and fraud, and it was accessed by an unauthorized actor and is at risk of acquisition and misuse. The risk of misuse is therefore imminent and substantial.[51]

102. The harm from the Data Breach will not necessarily manifest immediately. Stolen personal and health information may be held and trafficked for months or years before it is used, and a single set of stolen identifiers can be used repeatedly and in combination with other data to perpetrate multiple frauds over time. As a result, Plaintiff and the Class must remain vigilant, and bear the associated costs, for the foreseeable future.[52]

103. The reasonable and necessary response to this risk includes monitoring financial accounts and credit reports, placing and lifting fraud alerts and security freezes, reviewing medical

[51] U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2026).

[52] Ari Lazarus, Fed. Trade Comm'n, How Fast Will Identity Thieves Use Stolen Info? (May 24, 2017), https://consumer.ftc.gov/consumer-alerts/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited July 7, 2026).

and insurance records for evidence of medical identity theft, and purchasing credit-monitoring and identity-protection services. These measures impose real and ongoing costs of time and money on Plaintiff and the Class.[53]

VII. CLASS ACTION ALLEGATIONS

104. Plaintiff brings this action pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4) on behalf of the following proposed Class:

> All individuals residing in the United States whose private information was accessed, potentially accessed, or otherwise compromised as a result of the Data Breach that is the subject of this Complaint (the "Class").

105. Excluded from the Class are: Brown Health and its officers, directors, and affiliates; any entity in which Brown Health has a controlling interest; the judge presiding over this action and his or her immediate family and staff; and any person who timely and properly excludes himself or herself from the Class.

106. Plaintiff reserves the right to modify or amend the Class definition, including to add one or more subclasses, as discovery proceeds and the scope of the Data Breach is confirmed.

107. Numerosity (Rule 23(a)(1)). The Class consists of hundreds of thousands of individuals, including at least 290,357 residents of Massachusetts, along with residents of Rhode Island, Vermont, and other States, making joinder of all members impracticable. Class members are identifiable from Brown Health's own records.

108. Commonality (Rule 23(a)(2)). Common questions of law and fact exist as to all Class members and predominate over individualized questions, including, without limitation, the following:

[53] U.S. Gov't Accountability Off., Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737 (June 4, 2007), https://www.gao.gov/products/gao-07-737 (last visited July 7, 2026).

a. whether Brown Health collected and maintained the private information of Plaintiff and the Class;

b. whether Brown Health owed a duty to Plaintiff and the Class to implement and maintain reasonable measures to safeguard their private information;

c. whether Brown Health implemented and maintained reasonable data-security measures;

d. whether Brown Health's data-security practices met the standard of care reflected in HIPAA, in guidance from HHS and the FTC, in recognized frameworks published by NIST and CIS, and in the data-security laws of Massachusetts and Rhode Island;

e. whether Brown Health knew or should have known that its data-security measures were inadequate and that a breach was foreseeable;

f. whether Brown Health's conduct caused or permitted the Data Breach;

g. whether Brown Health entered into implied contracts with Plaintiff and the Class to safeguard their private information and, if so, whether Brown Health breached those contracts;

h. whether Brown Health was unjustly enriched by failing to provide the data security for which Plaintiff and the Class paid;

i. whether Brown Health provided timely and adequate notice of the Data Breach;

j. whether Plaintiff and the Class suffered injury as a result of the Data Breach and are entitled to damages;

k. whether Plaintiff and the Class are entitled to injunctive and other equitable relief, including a declaration of Brown Health's ongoing duties; and

l. the appropriate scope and terms of any injunctive relief necessary to protect the information that remains in Brown Health's possession.

109. Typicality (Rule 23(a)(3)). Plaintiff's claims are typical of the claims of the Class because Plaintiff and every Class member were affected by the same incident and the same alleged security failures, and their claims arise from the same course of conduct, Brown Health's failure to secure the private information entrusted to it, although the particular data elements affected and the resulting injuries may vary among Class members.

110. Adequacy (Rule 23(a)(4)). Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no interests antagonistic to those of the Class and has retained counsel experienced in complex class-action and data-breach litigation.

111. Predominance and Superiority (Rule 23(b)(3)). Common questions predominate over individualized ones, and a class action is superior to other methods for the fair and efficient adjudication of this controversy. The cost of litigating individual claims would exceed any individual recovery, and class treatment avoids the risk of inconsistent adjudications.

112. Injunctive Relief (Rule 23(b)(2)). Brown Health has acted or refused to act on grounds generally applicable to the Class, making final injunctive and corresponding declaratory relief appropriate for the Class as a whole.

113. Issue Certification (Rule 23(c)(4)). In the alternative, particular common issues, including the existence and breach of Brown Health's duty and the adequacy of its security and notice, are appropriate for issue certification.

VIII. CAUSES OF ACTION

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

114. Plaintiff incorporates by reference each preceding paragraph as if fully set forth herein.

115. Brown Health required Plaintiff and the Class to provide their private information as a condition of receiving healthcare services, and Brown Health collected, maintained, and controlled that information.

116. By collecting and storing this sensitive information, Brown Health assumed a duty to exercise reasonable care to secure and safeguard it, to prevent its unauthorized access and disclosure, and to implement processes to detect and respond to a breach and to provide prompt and accurate notice.

117. Brown Health's duty to use reasonable care arose from the special relationship between a healthcare provider and its patients, from Brown Health's voluntary undertaking to collect and safeguard the information, and from its position as the party in control of the information and best able to protect it against foreseeable criminal conduct.

118. The applicable standard of care is informed by well-established authorities, including the HIPAA Security Rule (referenced solely as a standard-of-care benchmark and not as an independent cause of action or a basis for negligence per se); guidance and frameworks published by the Department of Health and Human Services, the Federal Trade Commission, the National Institute of Standards and Technology, the Cybersecurity and Infrastructure Security Agency, and the Center for Internet Security; and the data-security standards reflected in Massachusetts law (M.G.L. c. 93H and 201 CMR 17.00) and Rhode Island law (R.I. Gen. Laws § 11-49.3-2).[54]

[54]U.S. Dep't of Health & Human Servs., Off. for Civil Rights, Security Rule Guidance Material, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited July 7, 2026).

119. Brown Health breached its duty of care by failing to implement and maintain reasonable security measures adequate to protect the private information in its custody, including, upon information and belief, by failing to adequately safeguard its systems against known threats, to monitor and detect unauthorized access, to timely remediate known vulnerabilities, and to maintain appropriate access controls and authentication.

120. It was reasonably foreseeable that Brown Health's failure to maintain reasonable security would result in the unauthorized access to Plaintiff's and the Class's private information and the resulting harm, particularly given the well-documented frequency of cyberattacks against healthcare providers.[55]

121. But for Brown Health's failure to exercise reasonable care, the private information of Plaintiff and the Class would not have been accessed and exposed. Brown Health's breach of its duty was the direct and proximate cause of the injuries suffered by Plaintiff and the Class.

122. As a direct and proximate result of Brown Health's negligence, Plaintiff and the Class have suffered and will suffer injury as described above, including the fraudulent charges incurred on Plaintiff's payment card, the compromise of their private information, the imminent risk of identity theft and fraud, lost time and out-of-pocket costs, the diminution in value of their private information, and the loss of the benefit of the bargain.

123. Plaintiff and the Class are entitled to compensatory and consequential damages, and to injunctive and equitable relief requiring Brown Health to adopt and maintain reasonable security measures and to provide adequate credit and identity monitoring.

COUNT II
BREACH OF IMPLIED CONTRACT

[55] Identity Theft Res. Ctr., 2025 Data Breach Report (Twentieth Edition) (Jan. 2026), https://www.idtheftcenter.org/wp-content/uploads/2026/01/2025-ITRC-Annual-Data-Breach-Report.pdf (last visited July 7, 2026).

(On Behalf of Plaintiff and the Class)

124. Plaintiff incorporates by reference each preceding paragraph as if fully set forth herein.

125. Plaintiff and the Class provided their private information to Brown Health as part of obtaining healthcare services from Brown Health. In exchange, Brown Health received the information and payment for its services, whether from Plaintiff and the Class directly or on their behalf.

126. Implicit in the parties' relationship was Brown Health's agreement to safeguard the private information it required Plaintiff and the Class to provide, to use that information only for authorized purposes, and to provide timely and accurate notice in the event of a breach.

127. The mutual understanding and intent that Brown Health would protect this information is demonstrated by the parties' conduct, by the sensitive and confidential nature of the information exchanged, and by Brown Health's obligations as a healthcare provider.

128. Plaintiff and the Class would not have entrusted their private information to Brown Health absent Brown Health's implied agreement to safeguard it.

129. Plaintiff and the Class performed their obligations under the implied contract by providing their information and paying for Brown Health's services.

130. Brown Health breached the implied contract by failing to implement reasonable data-security measures, by failing to safeguard the private information, and by failing to provide timely and adequate notice of the Data Breach.

131. As a direct and proximate result of Brown Health's breach, Plaintiff and the Class did not receive the full benefit of their bargain and instead received healthcare services of diminished value, and they suffered the injuries described above.

132. Plaintiff and the Class are entitled to compensatory, consequential, and nominal damages, and to appropriate injunctive and equitable relief.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class, in the Alternative)

133. Plaintiff incorporates by reference each preceding paragraph as if fully set forth herein. Plaintiff brings this Count in the alternative to the breach-of-implied-contract claim.

134. Plaintiff and the Class conferred a benefit on Brown Health by providing payment for services and by entrusting Brown Health with their valuable private information.

135. Brown Health appreciated and retained that benefit. A portion of the value Brown Health received was reasonably understood to be dedicated to providing adequate data security for the information entrusted to it.

136. Brown Health failed to provide the reasonable data security for which Plaintiff and the Class paid, and instead retained the benefit of the reduced costs realized by not implementing adequate safeguards.

137. Under these circumstances, it would be inequitable and unjust for Brown Health to retain the benefit it received without providing the data security that formed part of the consideration for the parties' exchange.

138. Plaintiff and the Class are entitled to restitution, disgorgement, or the imposition of a constructive trust in the amount by which Brown Health was unjustly enriched.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

139. Plaintiff incorporates by reference each preceding paragraph as if fully set forth herein.

140. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202, this Court may declare the rights and legal relations of the parties and grant further necessary or proper relief.

141. An actual controversy exists between Plaintiff and the Class, on the one hand, and Brown Health, on the other, concerning whether Brown Health owes ongoing duties to safeguard the private information that remains in its possession, whether Brown Health's existing data-security measures are reasonable and adequate, and whether Plaintiff and the Class remain at risk of further harm.

142. Brown Health continues to maintain the private information of Plaintiff and the Class, and, upon information and belief, has not demonstrated that it has fully remediated the deficiencies that permitted the Data Breach.

143. Plaintiff therefore seeks a declaration that (a) Brown Health owes a duty to Plaintiff and the Class to implement and maintain reasonable data-security measures; (b) Brown Health has not demonstrated that it has fully remediated the deficiencies that permitted the Data Breach; and (c) reasonable data-security measures, as specified in the Prayer for Relief, must be implemented and maintained.

144. A declaratory judgment is necessary and appropriate so that Plaintiff and the Class may ascertain their rights and so that Brown Health's continuing duties may be established and enforced.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court enter judgment against Brown Health and grant the following relief:

A. An order certifying the proposed Class, appointing Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. A declaration that Brown Health owes ongoing duties to safeguard the private information of Plaintiff and the Class and that its existing data-security measures are inadequate;

C. Injunctive and equitable relief requiring Brown Health to implement and maintain reasonable data-security measures, including, without limitation:

i. engaging independent third-party security auditors and internal personnel to conduct testing, including simulated attacks and penetration tests, on Brown Health's systems on a periodic basis;

ii. auditing, testing, and training Brown Health's security personnel regarding any new or modified procedures;

iii. encrypting private information maintained by Brown Health and implementing appropriate access controls, including multifactor authentication;

iv. segmenting data and implementing appropriate network monitoring, logging, and intrusion detection;

v. implementing a comprehensive information-security program with regular vulnerability scanning, timely patching, and threat management;

vi. conducting regular database scanning and security checks;

vii. routinely conducting internal training and education for employees on how to identify, contain, and respond to data-security threats;

viii. purging, deleting, and destroying private information no longer necessary for Brown Health's provision of services, in a reasonable manner;

ix. meaningfully educating Class members about the threats they face as a result of the Data Breach and the measures they can take to protect themselves;

x. implementing logging and monitoring sufficient to detect and track anomalous access to systems containing private information;

xi. engaging an independent third party to conduct periodic assessments of Brown Health's information-security program and to report the results to the Court and to Class Counsel for an appropriate period; and

xii. providing Class members with adequate credit monitoring and identity-theft protection, and the means to obtain reimbursement for losses fairly traceable to the Data Breach;

D. An award of damages, including actual, compensatory, consequential, and nominal damages, in an amount to be determined at trial;

E. An award of restitution and disgorgement as pleaded in the alternative;

F. An award of credit monitoring and identity-theft protection, and the costs of such monitoring, for an appropriate period;

G. An award of pre- and post-judgment interest as allowed by law;

H. An award of reasonable attorneys' fees, costs, and litigation expenses as allowed by law; and

I. Such other and further relief as the Court deems just and proper.

X. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims and issues so triable.

Dated: July 21, 2026

Respectfully submitted,

/s/Peter N. Wasylyk
Peter N. Wasylyk (RI Bar # 3351)
Law Offices of Peter N. Wasylyk
1307 Chalkstone Avenue
Providence, RI 02908
401-831-7730
Fax: 401-861-6064
Email: pnwlaw@aol.com

Scott J. Falgoust*
BRYSON HARRIS SUCIU & DEMAY PLLC
5301 Canal Boulevard
New Orleans, LA 70124
(919) 585-5634
sfalgoust@brysonpllc.com

**Application for admission pro hac vice forthcoming.*

Counsel for Plaintiff and the Class