

po

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss

SUPERIOR COURT
CIVIL ACTION

COMMONWEALTH OF MASSACHUSETTS,

Plaintiff,

v.

AVEANNA HEALTHCARE, LLC,

Defendant.

COMPLAINT

I. INTRODUCTION

1. The Commonwealth of Massachusetts, by and through its Attorney General, Maura Healey ("Commonwealth"), brings this action against Aveanna Healthcare LLC ("Aveanna") pursuant to the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the federal Health Information Technology for Economic and Clinical Health ("HITECH") Act, the Massachusetts Consumer Protection Act (G.L. c. 93A), and the Massachusetts Data Security Law (G.L. c. 93H).

2. Aveanna is a large pediatric and adult home healthcare provider with patients in 33 states nationwide, including Massachusetts, and which has been providing healthcare services for over 40 years.

3. At all relevant times, Aveanna collected and maintained patient and employee data on thousands of Massachusetts residents, including but not limited to, Social Security numbers, driver's license numbers, financial account numbers, and health information such as diagnoses,

medications, and treatment plans. As of September 2022, there are nine Aveanna offices in Massachusetts listed on the company website.

4. This case arises from a series of cyberattacks on Aveanna that took place in July and August of 2019, where attackers were able to access systems containing Aveanna patient and employee data (“the Data Breach”). The Data Breach was a series of “phishing” attacks— a practice whereby attackers send deceptive email messages to get employees to divulge information or to compromise network security. In such attacks, the attackers frequently impersonate company employees or other reputable businesses to instill trust in the message’s recipient.

5. As the “own[er] or licens[or]” of “personal information” (“PI”), Aveanna was required to safeguard this information from unauthorized access or unauthorized use under the Massachusetts Data Security Regulations (201 C.M.R. 17.00–17.05).

6. Aveanna failed to do so. Contrary to the requirements of the Data Security Regulations, Aveanna did not develop, implement, or maintain a sufficient written, comprehensive information security program (“WISP”) that encompassed the legally required administrative, technical, and physical safeguards.

7. Similarly, as a “covered entity” that maintained protected health information (“PHI”), Aveanna was required to safeguard this PHI in accordance with federal regulations promulgated under HIPAA.

8. Contrary to HIPAA regulations, Aveanna failed to implement appropriate security measures, procedures, and security awareness training.

9. By this action the Commonwealth seeks penalties, costs, and attorney’s fees, as available under G.L. c. 93A and G.L. c. 93H. The Commonwealth also seeks all necessary, appropriate,

and available equitable and injunctive relief to address, remedy, and prevent harm to Massachusetts residents resulting from the Defendant's actions and inaction.

II. THE PARTIES

10. The Plaintiff is the Commonwealth of Massachusetts, represented by its Attorney General, who brings this action in the public interest pursuant to G.L. c. 93A, § 4 and G.L. c. 93H, § 6.

11. Defendant Aveanna is a Delaware limited liability company with its principal place of business at 400 Interstate North Parkway SE, Atlanta, Georgia.

III. JURISDICTION, AUTHORITY, AND VENUE

12. The Attorney General is authorized to bring this action, in this Court, under G.L. c. 93A, § 4, G.L. c. 93H, § 6, and 42 U.S.C. § 1320d-5(d).

13. The HITECH Act § 13410(e), codified at 42 U.S.C. § 1320d-5(d), gives State Attorneys General the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules, codified at 45 C.F.R. §§ 160 and 164, respectively, to obtain damages on behalf of state residents, and to enjoin further violations of those Rules.

14. The Attorney General has provided notice of this action to the Secretary of Health and Human Services as required under 42 U.S.C. § 1320d-5(d)(4).

15. This Court has jurisdiction over the subject matter of this action by virtue of G.L. c. 93A, § 4 and G.L. c. 212, § 4.

16. This Court has personal jurisdiction over Aveanna under G.L. c. 223A, § 3, because, among other reasons, Aveanna has engaged in business and maintained at least nine offices in Massachusetts, and because Aveanna's actions and omissions have affected Massachusetts residents.

17. Venue is proper in Suffolk County under G.L. c. 223, § 5, as the Commonwealth is the plaintiff, and under G.L. c. 93A, § 4, because Aveanna has consented to venue in this court.

IV. FACTS

18. Aveanna is a national provider of pediatric and adult home health care. According to its website, Aveanna “cares for patients and families in 33 states through [its] rapidly growing network of more than 300 branch offices, offering a variety of care and services to more than 40,000 children and adults.” According to its website, as of September 2022, Aveanna has nine Massachusetts offices.

19. Aveanna provides or has provided home healthcare services to thousands of Massachusetts residents, including children under the age of 18.

20. At all relevant times, Aveanna was a “covered entity” within the meaning of 45 C.F.R. § 160.103, because it provided health care.

21. At all relevant times, Aveanna collected, maintained, or used Massachusetts residents’ protected health information (“PHI”), as defined by 45 C.F.R. § 160.103.

22. At all relevant times, Aveanna and its workforce were required to comply with the federal HIPAA standards that govern the privacy and security (45 C.F.R. Parts 160 and 164) of PHI.

23. At all relevant times, Aveanna owned or licensed personal information (“PI”) of Massachusetts residents within the scope of 201 C.M.R. 17.00–17.05 and G.L. c. 93H (together, the “Massachusetts Data Security Laws”).

24. As an owner or licensor of PI of Massachusetts residents, Aveanna was required, at all relevant times, to comply with the Massachusetts Data Security Laws.

The Data Breach

25. The Data Breach occurred in July and August of 2019 when Aveanna experienced a series of “phishing” cyberattacks.

26. A phishing attack is where attackers send fraudulent email messages in an effort to steal funds, obtain information, or gain access to an organization’s computer network. These messages are often designed to appear as though they are coming from legitimate senders.

27. Some phishing attacks will redirect a person to a fraudulent form where that person is asked to enter in their email username and password. This username and password are recorded and can then be used by the attacker to attempt to remotely login to that person’s email account to read and send emails, or to login to other applications where the same username and password are used.

28. In the Data Breach, the initial phishing attack began on or around July 9, 2019, with an email appearing to originate from a patient that was sent to Aveanna employees. At least one Aveanna employee provided their email username and password in response to this email, allowing outsiders to access the employee’s email account.

29. On or about July 24, 2019, a more sophisticated and personalized phishing attack, known as a spear-phishing attack, occurred. In this case, a customized email was sent to approximately 130 Aveanna employees, purporting to be from the President of Aveanna. The email requested that employees take an urgent survey by clicking on a link in the message. After clicking on the link, employees were asked to enter in their usernames and passwords to access the survey. The attack allowed the hackers to access more Aveanna employees’ accounts.

30. On or about July 26, 2019, more phishing emails were sent to Aveanna employees. This led to attempts to defraud employees by using the stolen credentials to login to an online human

resources system and alter the employees' direct deposit information in an effort to divert employee paychecks to the attackers.

31. The cyberattacks continued throughout August. From August 5, 2019 to August 24, 2019, the hackers sent approximately 650 additional phishing emails targeting Aveanna. These emails were sent from Aveanna employee email addresses.

32. Over the course of the attacks, over fifty employees from across the company responded to the phishing emails.

33. In letters dated February 14, 2020, Aveanna notified the Attorney General's Office and 4,084 affected Massachusetts residents of the Data Breach.

34. The types of information potentially impacted for residents included:

- a. Social Security numbers;
- b. driver's license or state identification card numbers;
- c. bank or financial account numbers;
- d. medical diagnoses, treatments, or conditions;
- e. medications; and
- f. insurance claims information.

Aveanna's Cybersecurity Plan

35. Prior to the Data Breach, in or about April 2019, Aveanna developed a phased plan for cybersecurity improvements. The plan noted a need to "establish significant baseline cyber security protections."

36. This plan acknowledged that "[s]ignificant cyber security risks" existed at Aveanna, particularly as its business was rapidly growing.

37. The plan also listed specific cybersecurity deficiencies, including, but not limited to:

- a. Limited ability to understand what devices, computers, and programs Aveanna has connected to its network;
- b. Limitations in scanning and assessment of systems and programs for cybersecurity vulnerabilities;
- c. Limited capabilities to detect an outsider within Aveanna's network, or to prevent such an outsider from getting into the network (commonly called Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), respectively);
- d. Limited use of centralized programs or devices to track potential cybersecurity events and Aveanna's responses to those events (commonly called Security Incident and Event Management (SIEM) systems);
- e. Inadequate tools to detect phishing attempts;
- f. Inadequate employee education about phishing attacks;
- g. Lack of the use of multifactor authentication (a method of signing into an account that uses both a password and an additional code or interface, typically viewed on a phone via either a text message or an application);
- h. Lack of knowledge of where all of Aveanna's sensitive data is located on Aveanna's network, and whether it is encrypted; and
- i. Insufficient auditing of those who had administrator access to Aveanna's network.

38. At the time of the Data Breach, implementation of the first phase of this cybersecurity plan had not been fully completed.

39. Following the Data Breach, and in connection with it, Aveanna engaged another company to review Aveanna's cybersecurity practices and procedures. As part of that review, a number of issues were noted, including:

- a. A lack of implementation of multi-factor authentication;
- b. A lack of visibility into Aveanna's own network, preventing Aveanna from understanding the extent of the Data Breach while it occurred;
- c. Failure to recognize or blacklist internet addresses that had poor email reputations;
- d. Poor firewall configurations;

40. In an internal presentation about the Data Breach, Aveanna acknowledged that its current cybersecurity posture was "lacking." Aveanna also noted that it lacked a SIEM and multi-factor authentication. Aveanna also committed to augment its employee training program concerning phishing.

41. Among other things, Aveanna purchased a SIEM and enabled multi-factor authentication after the Data Breach. Aveanna also enhanced its training with respect to phishing after the Data Breach.

V. CAUSES OF ACTION

COUNT I

Violations of HIPAA

42. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–41.

43. Aveanna is a covered entity within the meaning of HIPAA, and thus it and its workforce are required to comply with the HIPAA federal standards that govern the privacy and security of individually identifiable health information, 45 C.F.R. Part 160 and Subparts A, C, and E of Part 164.

44. Aveanna, as a covered entity, may only use or disclose PHI, as defined in 45 C.F.R. § 160.103, as expressly provided by HIPAA.

45. Furthermore, as noted in the HITECH Act, § 13410(e)(1) (codified at 42 U.S.C. § 1320d-5(d)(1)), in any case in which the attorney general of a State has reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates HIPAA, the attorney general of the State may bring a civil action on behalf of such residents to enjoin further such violations by the defendant and to obtain damages on behalf of such residents of the State.

46. By the actions alleged herein, Aveanna violated HIPAA by failing to comply with the standards, requirements, and implementation specifications as set forth in 45 C.F.R. § 164 of HIPAA, including by:

- a. failing to conduct accurate and thorough assessments of risks and vulnerabilities to the “confidentiality, integrity, and availability of electronic protected health information” it held, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A);
- b. failing to implement security measures, such as multi-factor authentication, to reduce these “risks and vulnerabilities to an appropriate level,” in violation of 45 C.F.R. 164.308(a)(1)(ii)(B);
- c. failing to “[i]mplement procedures to regularly review records of information system activity,” in violation of 45 C.F.R. 164.308(a)(1)(ii)(D); and
- d. failing to implement an adequate security awareness and training program in violation of 45 C.F.R. 164.308(a)(5)(i).

COUNT II

Violations of G.L. c. 93H/201 C.M.R. 17.00-17.05

47. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–
46.

48. The Commonwealth “may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of [c. 93H] and for other relief that may be appropriate.” G.L. c. 93H, § 6.

49. The Data Security Regulations, 201 C.M.R. 17.00-17.05, were promulgated under authority of G.L. c. 93H, § 2.

50. The Data Security Regulations “apply to all persons that own or license personal information about a resident of the Commonwealth.” 201 C.M.R. 17.01(2).

51. As a corporation, Aveanna is a “person” under the Data Security Regulations. *See* 201 C.M.R. 17.02.

52. The definition of “Personal Information” in the Data Security Regulations is coextensive to the definition of “Personal Information” in G.L. c. 93H, § 1. *See* 201 C.M.R. 17.02.

53. An entity “owns or licenses” personal information under the Data Security Regulations if it “receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.” 201 C.M.R. 17.02.

54. Aveanna is bound by the Data Security Regulations because at all relevant times, it owned or licensed personal information of at least one Massachusetts resident and continues to own or license the personal information of Massachusetts residents.

55. The Data Security Regulations “establish[] minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.” 201 C.M.R. 17.01(1).

56. Among these minimum standards is the duty of “[e]very person that owns or licenses personal information about a resident of the Commonwealth” to “develop, implement, and

maintain” a written information security program (a “WISP”) that “contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business . . . ; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information.” 201 C.M.R. 17.03(1).

57. The Data Security Regulations mandate certain specific minimum safeguards and obligations that an entity must develop, implement, and maintain in its WISP, including, among others:

- a. “Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic . . . records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks” (201 C.M.R. 17.03(2)(b));
- b. “[O]ngoing employee (including temporary and contract employee) training.” (201 C.M.R. 17.03(2)(b)(1));
- c. “[M]eans for detecting and preventing security system failures.” (201 C.M.R. 17.03(2)(b)(3)); and
- d. “Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.” (201 C.M.R. 17.03(2)(h)).

58. The WISP must also include the “the establishment and maintenance of a security system covering [the entity’s] computers, including any wireless system, that, at a minimum, and to the extent technically feasible,” contains, among other elements:

- a. “Secure user authentication protocols including: (a) control of user IDs and other identifiers; (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices” (201 C.M.R. 17.04(1));
- b. “Reasonable monitoring of systems, for unauthorized use of or access to personal information” (201 C.M.R. 17.04(4));
- c. “For files containing personal information on a system that is connected to the Internet, . . . reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information” (201 C.M.R. 17.04(6)); and
- d. “Education and training of employees on the proper use of the computer security system and the importance of personal information security.” (201 C.M.R. 17.04(8)).

59. Aveanna failed to develop, implement, and maintain its WISP and a security system covering its computers in such a way as to meet the minimum requirements of 201 C.M.R. 17.03 and 201 C.M.R. 17.04, including without limitation the minimum requirements set forth in 201 C.M.R. 17.03(2)(b), (2)(b)(1), (2)(b)(3), or (2)(h); or 201 C.M.R. 17.04(1), (4), (6), or (8).

60. Aveanna also failed to satisfy its obligations to develop, implement, and maintain a WISP that contained “administrative, technical, and physical safeguards that are appropriate” to:
(a) “the size, scope and type of business of” Aveanna; (b) “the amount of resources available to”

Aveanna; (c) the amount of data Aveanna stores; and (d) “the need for security and confidentiality of both consumer and employee information.” 201 C.M.R. 17.03(1).

61. These failures include, without limitation: not providing adequate education and training of employees on the proper use of the computer security system, not maintaining sufficient level of control over authorization and access to personal information, not implementing adequate procedures of vulnerability management and risk assessment; and not maintaining security systems sufficient to detect or prevent personal information compromise.

62. Accordingly, Aveanna violated G.L. c. 93H, § 2.

63. Each violation of the Data Security Regulations as to each affected Massachusetts resident is a separate violation of c. 93H, § 2.

COUNT III

Violations of G.L. c. 93A, § 2

64. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–63.

65. General Laws c. 93A, § 2(a) declares unlawful “unfair or deceptive acts or practices in the conduct of trade or commerce[.]”

66. Aveanna conducts trade and commerce in Massachusetts and with Massachusetts consumers.

67. As a corporation, Aveanna is a “person” under G.L. c. 93A, § 1(a).

68. Violations of HIPAA are violations of the Consumer Protection Act, G.L. c. 93A, § 2 by operation of 940 C.M.R. § 3.16(4).

69. Each of Aveanna's violations of G.L. c. 93H and 201 C.M.R. 17.00–17.05, as alleged herein and in Counts I & II, supra, are unfair or deceptive acts or practices in violation of G.L. c. 93A, § 2(a).

70. Accordingly, Aveanna violated G.L. c. 93A, § 2.

71. Each and every violation of HIPAA, G.L. c. 93H, and 201 C.M.R. 17.00–17.05 with respect to each Massachusetts consumer is a separate violation of G.L. c. 93A, § 2.

72. Aveanna knew or should have known that each of its violations of HIPAA, G.L. c. 93H, and 201 C.M.R. 17.00–17.05 would violate G.L. c. 93A, § 2.

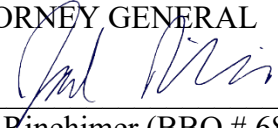
PRAYER FOR RELIEF

WHEREFORE, the Commonwealth requests that the Court grant the following relief:

1. Enter a permanent injunction prescribing appropriate relief;
2. Order that Aveanna pay civil penalties, restitution, and costs of investigation and litigation of this matter, including reasonable attorney's fees, to the Commonwealth of Massachusetts as provided for under G.L. c. 93A, § 4, and 42 U.S.C. § 1320d-5(d) in an amount to be determined at trial, and
3. Order such other just and proper legal and equitable relief.

COMMONWEALTH OF MASSACHUSETTS
MAURA HEALEY

ATTORNEY GENERAL

By: 

Jared Rinehimer (BBO # 684701)
Assistant Attorney General
Chief, Data Privacy and Security Division
One Ashburton Place, 18th Floor
Boston, MA 02108
617-727-2200
jared.rinehimer@mass.gov

Dated: October 27, 2022