

ATTORNEY GENERAL OF THE STATE OF NEW YORK  
BUREAU OF INTERNET & TECHNOLOGY

---

In the Matter of

Assurance No. 24-016

**Investigation by**  
**LETITIA JAMES,**  
**Attorney General of the State of New York, of**

**ALBANY ENT & ALLERGY SERVICES, P.C.,**

Respondent.

---

**ASSURANCE OF DISCONTINUANCE**

The Office of the New York State Attorney General (“OAG”) commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12), General Business Law (“GBL”) §§ 349, 899-aa, and 899-bb into two data security incidents at Albany ENT & Allergy Services, PC (“AENT” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of the OAG’s investigation and the relief agreed to by the OAG and Respondent, whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the “Parties”).

**OAG FINDINGS**

1. AENT is a multi-site medical practice in Albany, New York providing comprehensive care for patients with medical and surgical problems involving the ears, nose, and throat.
2. AENT does not have its own in-house information technology (“IT”) or information security (“InfoSec”) team. Rather, these functions are outsourced to third-party

vendors.

3. There is a single AENT employee who acts as a “liaison” to these third-party vendors “to implement recommended policies, procedures to ensure data quality, optimized system performance, and maintenance of security protocols.” This AENT employee has no IT or InfoSec experience or training.

4. Starting on or about March 23, 2023, and ending on April 4, 2023, Respondent’s information systems were infiltrated by two different threat actors. The first infiltration was discovered on March 27, 2023, when Respondent’s systems first displayed messaging associated with a ransomware attack. Respondent’s IT vendor immediately restored AENT’s systems after implementing some additional security measures. The IT vendor failed to identify the source of the breach before restoring external network access to AENT’s systems. The second infiltration was discovered on April 2, 2023, when Respondent’s systems displayed messaging from a different ransomware attacker. After the second incident, AENT hired a forensic cybersecurity firm which remediated any vulnerabilities before restoring it.

5. After the second breach, a forensic cybersecurity investigation concluded that the two different threat actors had been able to access AENT servers with various consumer information, including 213,935 patient records containing New Yorkers’ private information, as defined by New York’s breach notification law (New York General Business Law § 899-aa(1)(b)) (“PI”). The information exposed during the two incidents included name, date of birth, social security number, address, driver’s license numbers, diagnosis, conditions, lab results, medications, and other treatment information.

6. While the threat actors provided some evidence of exfiltrated data that include PI,

the ransoms were not paid. This decision followed the direction of the United States Government's Office of Foreign Asset Control's Updated Advisory dated September 21, 2021, which strongly discourages all private companies and citizens from paying ransomware demands. In response, both threat actors posted online data files exfiltrated from AENT containing the PI of New Yorkers.

7. AENT concluded its review of the incidents in May 2023 and, shortly thereafter, began notifying individuals in accordance with New York law. AENT also offered one year of free credit monitoring to affected individuals. Additionally, AENT issued substitute notice and media notice in five states.

8. AENT was unable to confirm the attack vector in part because it did not retain server logs for a reasonable period of time and AENT did not have security programs in place to monitor and analyze server traffic. However, the forensic cybersecurity consultant concluded that the threat actors likely gained access to AENT's systems through exploitation of a vulnerability in AENT's Cisco VPN firewall.

#### The OAG Investigation Finds More Private Information Exposed

9. On May 25, 2023, AENT reported to OAG, as required by GBL § 899-aa, that 120,459 New Yorker social security numbers were exposed in the two incidents. However, during its investigation, the OAG discovered PDF copies of New York driver license numbers in the data files posted online by the threat actors. After the OAG brought this inaccuracy to AENT's attention, AENT amended its notice to include 80,127 NYS drivers' license numbers.

10. In the course of its investigation, the OAG discovered that the threat actors had accessed six AENT devices that hosted unencrypted PI and that some of these devices continued

to host unencrypted PI for months after the breaches. After the OAG addressed this issue with AENT, AENT took steps to remediate the unprotected personal information remaining on its systems. AENT had an encryption policy for laptop computers, but it had no encryption policy covering PI on its other systems. Similarly, AENT multi-factor authentication (“MFA”) requirements were not adopted for all systems, including certain remote access systems. .

11. The OAG’s investigation identified numerous inadequacies in AENT’s data security including failure to:

- a. adequately monitor vendors responsible for outsourced IT and InfoSec functions;
- b. adopt a data encryption policy and train employees regarding the importance of encrypting PI;
- c. identify and encrypt PI, including database backups;
- d. timely install critical software security updates;
- e. implement reasonable network security processes, including network logging, log monitoring, log analysis, log repositories, IP restrictions, and intrusion detection technology;
- f. adequately identify, inventory, and protect PI before the attacks;
- g. adequately identify, inventory, and remediate unencrypted copies of PI after the attacks;
- h. meet minimum requirements for password security;
- i. adopt a multifactor authentication policy (“MFA”) to access its local server environment and online services reached through its local server

environment;

- j. adequately control administrator privileges;
- k. implement reasonable security testing, including penetration tests and vulnerability tests;
- l. accurately perform security risks analyses; and
- m. follow security risk analysis recommendations.

12. Based on the foregoing, the OAG has determined that AENT violated Executive Law § 63(12) and GBL §§ 349, 899-aa, and 899-bb.

13. Respondent neither admits nor denies the OAG's Findings, paragraphs 1-12 above.

14. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12), and GBL §§ 349, 899-aa, and 899-bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

**PROSPECTIVE RELIEF**

**GENERAL COMPLIANCE**

15. AENT shall comply with Executive Law § 63(12), GBL §§ 349, 899-aa, and 899-bb, in connection with its collection, use, and maintenance of PI, and shall maintain reasonable security policies and procedures designed to safeguard PI from unauthorized use or disclosure.

16. Respondent shall provide notice of the requirements of the Assurance to all

management-level employees, owners, investors, and/or Board members and shall implement appropriate training of such individuals. The notice and training required under this paragraph shall be provided to the appropriate individuals within sixty (60) days of the effective date of the AOD, or within thirty (30) days of starting such position.

### **INFORMATION SECURITY PROGRAM**

17. AENT shall maintain a comprehensive Information Security Program that is reasonably designed to protect the security, integrity, and confidentiality of PI that Respondent collects, stores, transmits, and/or maintains. Respondent shall document in writing, not less than annually, the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, incorporate the processes in paragraphs 19 - 26, which shall be performed and/or updated at least annually, including:

- a. Assess internal and external risks to the security, integrity, and confidentiality of PI;
- b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that are appropriate to: (i) the size and complexity of Respondent's operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the PI that Respondent collects, stores, transmits, and/or maintains.
- c. Assess the sufficiency of any safeguards in place to address the internal and external risks Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with (b) above;

d. Test and monitor the effectiveness of the safeguards and modify the Information Security Program based on the results to ensure the safeguards comply with (b) above;

e. Select service providers capable of appropriately safeguarding PI, contractually require service providers to implement and maintain appropriate safeguards to protect PI, and take appropriate steps to verify service providers are complying with the contractual requirements; and

f. Evaluate the Information Security Program and adjust the Program in light of any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Program.

18. Respondent shall appoint a qualified individual to be responsible for implementing, maintaining, and monitoring the Information Security Program. The appointed individual shall have credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, and monitoring the Information Security Program. The appointed individual shall report in writing at a minimum semi-annually to the Chief Executive Officer, senior management, and the Board of Directors or equivalent governing body, or an appropriate committee thereof, concerning Respondent's security posture, the security risks faced by Respondent, and the Information Security Program.

#### **SPECIFIC INFORMATION SAFEGUARDS AND CONTROLS**

19. Encryption of Data: Respondent shall at least annually inventory all PI on its network, systems, and devices. Respondent shall ensure the PI that it collects, stores, transmits,

and/or maintains is encrypted using an encryption method appropriate to the sensitivity of the PI. Nothing in this paragraph requires Respondent to (i) individually identify each type of PI contained on its network, system, or devices, so long as the encryption method used for such PI assumes it is the highest level of sensitivity or (ii) encrypt individual files on a device that is itself encrypted.

20. Monitoring and Logging: Respondent shall implement reasonable controls to monitor and log all security and operational activity related to networks, systems, and devices, and establish and maintain policies and procedures to regularly review appropriate records for anomalous activity. Respondent shall store logs of events that indicate anomalous activity for a period of time that is sufficient to detect, investigate, and respond to security incidents.

21. Critical Updates: Respondent shall implement reasonable policies and procedures to ensure that critical security updates are installed promptly across its network, systems, and devices. Respondent shall regularly audit that process to ensure compliance.

22. Access and Authentication Controls: Respondent shall establish, implement, and maintain policies and procedures to appropriately limit access to PI. The policies and procedures shall require, at a minimum:

- a. Granting individuals and organizations access only to those resources and data that are necessary for their business functions;
- b. Promptly removing individuals' and organizations' access to resources and data upon separation or, upon an individual's change in responsibilities, promptly removing the individual's access to resources and data that are no longer required to discharge those responsibilities;



- c. Requiring completion of multifactor authentication to remotely access resources and data, including when accessed from within Respondent's local environment; and
- d. Following up-to-date minimum requirements for password creation, protection, and rotation.

23. Vendor Risk Management: AENT shall maintain and implement reasonable written policies and procedures to oversee IT and InfoSec vendor performance of any security functions and/or PI privacy obligations (arising by contract or law). AENT shall utilize a variety of security assessment and monitoring practices to confirm that such vendors are able to comply with AENT's security and privacy obligations.

#### **INFORMATION SECURITY PROGRAM ASSESSMENTS**

24. Within one (1) year of the effective date of this Assurance, Respondent shall obtain a comprehensive assessment of the information security of Respondent's network, systems, and devices conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession. Such assessment shall be documented (a "Third-Party Assessment Report") and provided to the OAG within two weeks of completion. Annually for five (5) years thereafter, Respondent shall obtain Third-Party Assessment Reports which Respondent shall maintain for seven (7) years from the date of each Third-Party Assessment Report and shall provide to the OAG upon request. The Third-Party Assessment Reports shall:

- a. Identify the specific administrative, technical, and physical safeguards maintained by Respondent's Information Security Program;
- b. Document the extent to which the identified administrative, technical, and

physical safeguards are appropriate considering Respondent's size and complexity, the nature and scope of Respondent's activities, the reasonably anticipated risks, and the sensitivity of the PI maintained on Respondent's network, systems, and devices; and

c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondent meet the requirements of the Information Security Program and the Assurance.

### **PERSONAL INFORMATION PROTECTION**

25. Respondent shall either (i) delete all the personal information collected from its patients or (ii) encrypt or otherwise obfuscate the personal information it retains.

### **INCIDENT RESPONSE**

26. Respondent shall establish, implement, and maintain a comprehensive incident response plan. The incident response plan shall be documented in writing and include, at a minimum, the following policies:

a. If Respondent has reason to believe that there has been unauthorized access to or the acquisition of PI owned, licensed, or maintained by the Respondent (a "Security Event"), Respondent shall promptly conduct a reasonable investigation to determine, at a minimum, whether PI was accessed or acquired without authorization, and, if so, what PI was accessed or acquired.

b. If Respondent determines PI has been, or is reasonably likely to have been, accessed or acquired without authorization, Respondent shall expediently provide each consumer whose PI has been, or is reasonably believed to have been,

accessed or acquired without authorization, by email or letter or other legally valid forms of substitute notice established under New York law, material information concerning the security event that is reasonably individualized to the customer including, at a minimum, the timing of the security event, whether the PI was accessed or acquired without authorization, what PI was accessed or acquired, and what actions have been taken to protect the consumer. If necessary, in order to provide expedient notice to consumers, Respondent may provide more than one notice that collectively provide all material information.

#### **OAG ACCESS TO RECORDS**

27. Unless otherwise provided for in this Assurance, Respondent shall retain the documentation and reports required by paragraphs 17 - 24 and paragraph 26 for at least six years. Such documentation and reports shall be made available to the OAG within fourteen (14) days of a written request from the OAG. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any other claim.

#### **MONETARY RELIEF**

28. Respondent shall pay to the State of New York one million dollars (\$1,000,000) in civil penalties and costs as follows:

- a. A payment of two hundred and fifty thousand dollars (\$250,000) shall be made in full within sixty (60) days of the date of this Assurance;
- b. A payment of two hundred and fifty thousand dollars (\$250,000) shall be made no later than August 31, 2025;

c. Five hundred thousand dollars (\$500,000) shall be suspended; provided, however, that the suspended amount will be immediately due and payable if the OAG finds that Respondent fails to spend at least four hundred fifty thousand dollars (\$450,000) to enhance and maintain its information security program in each of the five fiscal years following the execution of this Assurance.

Payments to the OAG shall be made by wire transfer in accordance with instructions provided by a OAG representative and shall reference AOD No. 24-016.

### **MISCELLANEOUS**

29. Respondent expressly agrees and acknowledges that the OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 37, and agrees and acknowledges that in such event:

a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;

b. the OAG may use statements, documents or other materials produced or provided by the Respondent prior to or after the effective date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue.

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

30. If a court of competent jurisdiction determines that the Respondent has violated

the Assurance, the Respondent shall pay to the OAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

31. This Assurance is not intended for use by any third party in any other proceeding.

32. Acceptance of this Assurance by the OAG is not an approval or endorsement by OAG of any of Respondent's policies, practices, or procedures, and the Respondent shall make no representation to the contrary.

33. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondent. Respondent shall include any such successor, assignment, or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the OAG.

34. Any failure by the OAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by the Respondent.

35. Nothing contained herein shall be construed as to deprive any person of any private right under law.

36. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 24-016, and shall be in writing and shall, unless

expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to the Respondent, to:

Gavin Setzen, MD  
President & CEO  
Albany ENT & Allergy Services, PC  
123 Everett Rd  
Albany, NY 12205

If to the OAG, to:

Bureau Chief  
Bureau of Internet & Technology  
28 Liberty Street  
New York, NY 10005

37. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondent and their counsel and the OAG's own factual investigation as set forth in Findings, paragraphs 1-12 above. The Respondent represents and warrants that neither it nor its counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

38. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondent in agreeing to this Assurance.

39. The Respondent represents and warrants, through the signatures below, that the

terms and conditions of this Assurance are duly approved. Respondent further represents and warrants that AENT, by Gavin Setzen, MD, as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of AENT.

40. Respondent agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis.

41. Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that the Respondent violates the Assurance after its effective date.

42. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

43. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

44. Respondent acknowledges that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

45. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

46. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.


47. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties,


notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned, and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

48. The effective date of this Assurance shall be November 1, 2024.

LETITIA JAMES  
Attorney General of the State of New York  
28 Liberty Street  
New York, NY 10005

ALBANY ENT & ALLERGY  
SERVICES, P.C.  
123 Everett Rd  
Albany, NY 12205

By:   
Gena Feist  
Assistant Attorney General  
Bureau of Internet & Technology

By:   
Gavin Setzen, MD  
President & CEO  
Albany ENT & Allergy Services, PC

Date: 10/29/24

Date: 10/22/2024