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

In the Matter of

Assurance No. 24-086

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

HealthAlliance, Inc.

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("OAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") § 899-bb into a data security incident at HealthAlliance, Inc. ("HealthAlliance" or "Respondent"). This Assurance of Discontinuance ("Assurance") contains the findings of OAG's investigation and the relief agreed to by the OAG and HealthAlliance whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the "Parties").

FINDINGS OF OAG

1. HealthAlliance is a New York not-for-profit corporation that operates healthcare facilities in Ulster and Delaware Counties, New York, including, HealthAlliance Hospital in Kingston, Margaretville Hospital in Margaretville, and Mountainside Residential Care Center in Margaretville.

2. HealthAlliance utilizes telemedicine to connect patients with providers with the relevant medical expertise in other areas of the state virtually. To facilitate critical telemedicine services, HealthAlliance deployed a suite of networking products known as NetScaler provided

by Citrix so these providers can securely and remotely connect HealthAlliance's network to support and deliver critical health care services.

3. On July 18, 2023, Citrix released cybersecurity advisory for CVE-2023-3466, CVE-2023-3467, and CVE-2023-3519 along with patches for those vulnerabilities. CVE-2023-3519 related to a critical zero-day vulnerability affecting two NetScaler products deployed on HealthAlliance's network. According to the advisory, threat actors had exploited this vulnerability to deploy a web shell and thereby gain unauthorized access to an organization's critical infrastructure. The web shell enabled threat actors to perform discovery on the victim's Active Directory and collect and exfiltrate Active Directory user account data.

4. Following the release of the advisory for CVE-2023-3466, CVE-2023-3467, and CVE-2023-3519, HealthAlliance immediately initiated its patch management protocol, which dictated that, in order to prevent a service disruption, patches be applied to standby appliances before being deployed in the production environment.

5. Due to technical issues, HealthAlliance was unable to successfully apply the patch for CVE-2023-3519 to a standby appliance. When HealthAlliance attempted to apply the patch, the patch would not install successfully.

6. Two days after its unsuccessful attempts to apply the patch for CVE-2023-3519, HealthAlliance contacted Citrix for support but Citrix was unable to help HealthAlliance successfully apply the patch.

7. After numerous attempts to apply the patch to a standby appliance, HealthAlliance engaged other third-party experts, to try to resolve the issue, but was unsuccessful.

8. HealthAlliance worked diligently with third-party experts throughout the summer and into the fall, to troubleshoot the technical issue on a standby appliance while keeping the NetScaler appliance online to avoid disruptions to the provision of telemedicine services.

9. On October 12, 2023, threat actors emailed several HealthAlliance leadership members, claiming they had gained access to HealthAlliance's network and had stolen sensitive data, including patient records and employee information.

10. On or around that time, HealthAlliance also became aware of unusual activity in its IT systems. In response, HealthAlliance launched an investigation and notified law enforcement.

11. To secure its systems and to prevent any further unauthorized access, HealthAlliance took them all offline temporarily and replaced the NetScaler appliances with new ones and notified affected physicians and patients of the resultant service disruption.

12. HealthAlliance's investigation determined that a threat actor had exploited the NetScaler vulnerability set forth in advisory CVE-2023-3519 and used a web shell to harvest credentials from the NetScaler appliance.

13. The investigation further revealed that the threat actors had used the harvested credentials to access over forty different hosts within the network and, that between September 22, 2023 and October 8, 2023, the threat actors exfiltrated 196 gigabytes of data.

14. The exfiltrated data included patient Social Security numbers that had been stored, in contravention of HealthAlliance's data security policy, in unencrypted files.

15. HealthAlliance determined that the exfiltrated data included personal information of 237,733 New York residents. In the majority of cases, the exfiltrated patient data included patient name, address, date of birth, Social Security number, diagnosis, lab results, medications,

and other treatment information, health insurance information, provider name, dates of treatment, and/or financial information.

16. Financial and medical data without Social Security numbers was also exfiltrated for another 17,326 patients..[1]

17. On December 11, 2023, following a forensic review of the incident, HealthAlliance mailed notice letters to 242,641 HealthAlliance patients who are New York residents and offered complimentary credit monitoring and identity protection services to individuals whose Social Security numbers may have been involved.

The OAG Finds Respondent's Conduct Violated New York Law

18. Executive Law § 63(12) prohibits illegal practices in the conduct of any business.

19. GBL § 899-bb requires any person or business that owns or licenses computerized data which includes the private information of a resident of New York to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information. "Private information" includes Social Security numbers and financial information, when such data is obtained in combination with the patient's name or personal identifier. GBL §§ 899(bb)(1)(b), 899-aa(1)(b).

20. The OAG finds that Respondent's conduct violated Executive Law § 63(12) and GBL § 899-bb.

21. Respondent neither admits nor denies the OAG's Findings, in paragraphs 1-17 above.

---

22. 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 § 899-bb based on the conduct described above.

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

RELIEF

23. For the purposes of this Assurance, the following definitions shall apply:

a. "Affected Consumer" shall mean any person whose Personal Information was subject to the Security Event. "Private Information" means private information as defined in New York General Business Law § 899-aa(1)(b).

b. "Security Event" means the unauthorized access to and acquisition of Private Information stored on Respondent's network described in paragraphs 1-17 above.

GENERAL COMPLIANCE

24. Respondent shall comply with Executive Law § 63(12) and GBL § 899-bb in connection with its collection, use, and maintenance of Private Information.

INFORMATION SECURITY PROGRAM

25. Respondent shall maintain a written information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Private Information that Respondent collects, stores, transmits, and/or maintains. Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include all of the requirements detailed in paragraphs 28-37 and the following processes:

a. Assess, update, and document, at least annually, internal and external risks

to the security, integrity and confidentiality of Private Information, including but not limited to all entries in the most recent Data Inventory, as defined in paragraph 28;

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 Private Information that Respondent collects, stores, transmits, and/or maintains;

c. Assess and document, at least annually, the sufficiency of any safeguards in place to address the internal and external risks to Private Information Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with this Assurance;

d. Test and monitor the effectiveness of such safeguards at least annually, and modify the Information Security Program based on the results to ensure the safeguards comply with this Assurance;

e. Assess and document, at least annually, 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; and

f. Take reasonable steps to select service providers capable of reasonably safeguarding Private Information, contractually require service providers to implement and maintain reasonable safeguards to protect Private Information and take reasonable steps to verify service providers are complying with the contractual requirements.

26. Respondent shall designate a qualified employee responsible for implementing,

maintaining, assessing, updating, and monitoring the Information Security Program. The designated employee shall have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, assessing, updating, and monitoring the Information Security Program. The designated employee shall report at least quarterly to Respondent's Chief Executive Officer (or the equivalent thereof) and at least semi-annually to the Board of Directors (or an appropriately designated Board Committee) concerning Respondent's Information Security Program. Such reports shall be in writing and include but not be limited to the following: the staffing and budgetary sufficiency of the Information Security Program, the degree to which the Information Security Program has been implemented, challenges to the success of the Information Security Program, the existing and emerging security risks faced by Respondent, and any barriers to the success of the Information Security Program.

27. Respondent shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, assessing, updating, or monitoring the Information Security Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within one-hundred-and twenty (120) days of the Effective Date of this Assurance, or within thirty (30) days of when an employee first assumes new responsibility for implementing, maintaining, assessing, updating, or monitoring the Information Security Program. Respondent shall document that it has provided the notices and training required in this paragraph.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

28. Data Inventory: Within sixty (60) days of the Effective Date of this Assurance, to

the extent it has not already done so, Respondent shall develop and maintain a Data Inventory of all instances in which it transmits, Private Information to third-party vendors. Respondent shall update and document its Data Inventory not less than annually. The Data Inventory shall, at a minimum, include the following processes:

a. Identify all points at which Private Information is transmitted to third-party vendors;

b. Ensure that third-party vendors use reasonable safeguards to protect Private Information at all times, including but not limited to appropriate encryption, masking, obfuscation, and other methods of rendering Private Information incomprehensible and/or inaccessible.

29. Respondent shall conduct a semi-annual audit of the Data Inventory to ensure that all Private Information shared with third-party vendors is stored in accordance with its data security and privacy policies.

30. Respondent shall utilize tools to periodically perform data classification to identify Private Information stored on network file shares. The tools shall generate reports for the information security team to review in order to identify data that should be removed or further secured.

31. Respondent shall provide training and periodic reminders to workforce members on Respondent's policies and procedures regarding the creation and maintenance of files containing Private Information.

32. Patch Management for Critical Vulnerability: Consistent with its existing patch management policy, Respondent shall implement patches for vulnerabilities identified as critical for the Respondent's business operations within 72 hours. In instances where Respondent is unable to patch such a vulnerability within 72 hours, Respondent must neutralize the vulnerability with compensating controls, if available, as soon as possible, asset replacement, or termination of services until appropriate security measures are in place to mitigate the risk. To the extent suspension or termination of services is necessary, nothing in this provision requires Respondents to take any actions or deploy any measures that would compromise critical patient care services.

33. Respondent shall update its patch management policy to define the software vulnerability risk scenarios requiring patch management, including:

a. Routine Patching (Standard procedures for patches that are regularly released);

b. Emergency Patching (Procedures for addressing severe vulnerabilities or those being actively exploited);

c. Emergency mitigation (Procedures for crisis situations to temporarily mitigate vulnerabilities before a patch is available. May be required if a patch is flawed, disrupts other systems, or is compromised); and

d. Unpatchable assets (Implementation of asset isolation or other methods to mitigate the risk of systems that cannot be easily patched. Typically required if routine patching cannot accommodate these systems within a reasonable timeframe).

34. Restriction of Unnecessary Lateral Communications: Respondent shall adopt appropriate security measures to separate web applications services from the organization's intranet.

35. Respondent shall implement a virtual local area network ("VLAN") segmentation.

36. Malicious IP Address Blacklisting: Respondent shall maintain an updated threat feed and block known malicious IP addresses from connecting to the organization's infrastructure.

37. Monitoring: Respondents shall maintain a system designed to collect and monitor file access activity as well as activity on any platforms or applications that employ Active Directory authentication operated by Respondent that collect, store, transmit, or maintain Private Information. Respondent shall also establish and maintain reasonable policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (i) provide for centralized logging and monitoring that includes collection and aggregation of logging for Respondent's file access activity and any platforms or applications that employ Active Directory authentication operated by Respondent that collect, store, transmit, or maintain Private Information, and (ii) monitor for and alert security personnel to suspicious activity. Activity logs should be immediately accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

OAG ACCESS TO RECORDS

38. Respondent shall retain the documentation and reports required by paragraphs 25-28, and 33 for at least six years. Such documentation and reports shall be made available to the OAG within fourteen (14) business 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.

IDENTITY THEFT PROTECTION FOR AFFECTED CONSUMERS

39. To the extent not already completed, Respondent shall offer Affected Consumers the opportunity to enroll in the following identity monitoring services at no cost for an aggregate one (1) year:

a. Credit Monitoring: Daily Credit Report monitoring from a nationwide consumer reporting agency (i.e., Equifax Information Services LLC, Experian Information Solutions, Inc., or TransUnion LLC) showing key changes to an Affected Consumer's Credit Report including automated alerts where the following occur: new accounts are opened; inquiries or requests for an Affected Consumer's Credit Report for the purpose of obtaining credit; changes to an Affected Consumer's address; and negative information, such as delinquencies or bankruptcies.

b. Fraud Consultation and Identity Theft Restoration: provide live support and explanation of the identity theft restoration process to ensure the victim understands his or her rights and responsibilities; investigate and resolve complicated trails of fraudulent activity; issue fraud alerts for the victim with the three consumer credit reporting agencies, the Social Security Administration, the Federal Trade Commission and the U.S. Postal Service; prepare appropriate documentation, from dispute letters to defensible complaints;

work all identity theft issues until they have been verifiably resolved with all the organizations impacted including financial institutions, collections agencies, check clearinghouse companies, landlords, property managers, and government entities; and

c. Social Security Number trace for minors.

MONETARY RELIEF

40. Respondent shall pay to the State of New York one million four hundred thousand dollars ($1,400,000) in civil penalties and costs as follows:

a. A payment of five hundred and fifty thousand dollars ($550,000) shall be made in full within sixty (60) days of the date of this Assurance;

b. Eight hundred fifty thousand dollars ($850,000) shall be suspended; provided, however, that the suspended amount will be immediately due and payable if the NYAG finds that any of the materials submitted to the OAG during this settlement process relating to Respondent's financial well being contained any material misrepresentations.

41. Payments shall be made by wire transfer in accordance with instructions provided by a OAG representative and shall reference Assurance No. 24-086.

MISCELLANEOUS

42. 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 49 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).

43. 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.

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

45. 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.

46. 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 prior written consent of the OAG, which shall not be unreasonably withheld.

47. 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.

48. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 24-086, 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: Christopher J. Librandi, or in his/her absence, to the person holding the title of Senior Vice President, Deputy General Counsel.
>
> If to the OAG, to: Marc Montgomery, or in his/her absence, to the person holding the title of Bureau Chief, Internet and Technology Bureau.

49. 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 1-17 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.

50. 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.

51. 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 HealthAlliance, Inc., by the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of HealthAlliance, Inc.

52. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

53. 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 basisNothing in this paragraph affects Respondent's right to take legal or factual positions in defense of litigation or other legal proceedings to which the NYAG is not a party.

54. 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.

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

56. 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.

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

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

59. 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.

60. 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.

61. The effective date of this Assurance shall be November 20, 2024.

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

By: _____
Marc Montgomery
Assistant Attorney General
Bureau of Internet & Technology

Date: _____

Health Alliance, Inc.

By: Michael D Israel
Michael D. Israel
President and Chief Executive Officer, WMCHealth

Date: 12/2/2024