ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance ("Assurance") is entered into by the Attorneys General of Oregon and Utah (collectively "Attorneys General") and Avalon Healthcare Management, Inc. ("Avalon"). This Assurance constitutes a good faith settlement between Avalon and the Attorneys General of the claims related to the 2019 data breach, in which a person or persons gained unauthorized access to an Avalon employee's email account that contained personally identifiable information ("PII") and protected health information ("PHI"), and Avalon failed to provide timely notice to the Attorneys General.

In consideration of their mutual agreements to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

INTRODUCTION

1. This Assurance resolves the State of Utah's concerns that Avalon violated the Utah Protection of Personal Information Act, Utah Code §§ 13-44-101 et seq. (the "UPPIA"), and the Utah Consumer Sales Practices Act, Utah Code §§ 13-11-1 et seq (the "UCSPA").

2. This Assurance is not an admission or finding that Avalon violated the UPPIA or the UCSPA. Avalon has agreed to enter this Assurance and settlement of contested matters to avoid further controversy and expense.

3. Avalon is a Utah corporation with care facilities located in California, Hawaii, Nevada, Oregon, Utah, and Washington.

4. The State of Utah is represented by Sean D. Reyes, Utah Attorney General. The Attorney General is authorized to enforce the UPPIA and is authorized as counsel to the Utah Division of Consumer Protection to enforce the UCSPA.

DEFINITIONS

5. "Consumer" shall mean an individual resident of the Attorneys General's states.

6. "Consumer Protection Laws" shall mean ORS 646.605 et seq., and Utah Code §§ 13-11-1 et seq.

7. "Covered Systems" shall mean components, such as servers, workstations, and devices, within the Avalon Network that are routinely used to collect, process, communicate, and/or store PI and/or PHI.

8. "Data Breach" shall mean the security incident Avalon became aware of in July 2019, and publicly announced in March 2020, in which a person or persons gained unauthorized access to an Avalon employee's email account that contained PI and PHI, and which impacted approximately 14,500 individuals nationwide.

9. "Data Breach Notification Laws" shall mean ORS 646A.600 et seq., and Utah Code § 13-44-202.

10. "Data Security Incident" shall mean any event that (i) results in the unauthorized access, acquisition, or exfiltration of electronic PI or PHI collected, process, transmitted, stored, or disposed of by Avalon, or (ii) causes lack of availability of electronic PI or PHI of at least 500 consumers nationwide.

11. "Effective Date" shall be immediately upon execution by Avalon of this Assurance.

12. "Encrypt" or "Encryption" shall refer to the transformation of data at rest or in transit into a form in which meaning cannot be assigned without the use of confidential process.

13. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services ("HHS") Regulations, 45 C.F.R. §§ 160 et seq.

14. "Multi-Factor Authentication" means authentication through verification of at least two of the following authentication factors: (i) knowledge factors, such as a password, (ii)

possession factors, such as a token, connection through a known authenticate source, or a text message on a mobile phone, or (iii) inherent factors, such as biometric characteristics.

15. "Network" shall mean all networking equipment, databases or data stores, applications, servers and endpoints that are capable of using and sharing software, data and hardware resources, and that are owned, operated, and/or controlled by Avalon.

16. "Personal Information" or "PI" shall mean the data elements in the definitions found in ORS 646A.06 and Utah Code § 13-44-102.

17. "Protected Health Information" or "PHI" shall mean the elements in the definition found in 45 C.F.R. § 160.103.

18. "Security Rules" shall mean the HIPAA Regulations that establish national standards to safeguard individuals' electronic PHI that is created, received, used, or maintained by a Covered Entity or business associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

ASSURANCES

19. Avalon shall comply with the Consumer Protection Laws and HIPAA by adopting reasonable data security practices to adequately protect the security, confidentiality, and integrity of all PI and PHI which Avalon collects, uses, and maintains, as well as by complying with the reporting and notification requirements set forth in the Data Breach Notification Laws.

20. Avalon agrees to adhere to each of the following requirements:

(a) **Data Security Incident Response Plan**. Within sixty (60) days of the Effective Date, Avalon shall develop, implement, and maintain a Data Security Incident response plan that includes the following:

(i) Identify the types of incidents that fall within the scope of the plan, which must include any incident that Avalon reasonably believes might indicate a Data Security Incident;

(ii) Describe all individuals' roles in fulfilling responsibilities under the plan, including back-up contacts and escalation pathways;

(iii) Establish a process for investigating information indicating that a Data Security Incident may have occurred;

(iv) Require regular testing and review of the plan. Based on testing and review, Avalon shall re-evaluate and revise the plan as is reasonable or necessary; and

(v) Maintain a report that includes a description of any Data Security Incident that does not trigger notice under the Data Breach Notification Laws, Avalon's response to the Data Security Incident and why Avalon determined that the Data Security Incident did not trigger notice under the Data Breach Notification Laws. Avalon must retain the report for seven (7) years and make the report available to the Attorneys General upon request.

(b) **Information Security Program.** Within sixty (60) days of the Effective Date, Avalon shall develop, implement, and maintain a comprehensive written information security program ("Information Security Program") that includes at least the security requirements set forth in paragraph 21(b)(i) – (viii) of this assurance. Avalon shall review the Information Security Plan not less than annually and make any updates necessary to ensure the reasonable protection of the security, integrity, and confidentiality of PI and PHI that Avalon collects, stores, transmits, and maintains. The Information Security Program is permitted to simultaneously comply with this section and section 21(f) addressing HIPAA compliance.

(i) Safeguards: The Information Security Program shall comply with any applicable requirements under the Consumer Protection Laws and the Data Breach Notification Laws and shall contain administrative, technical, and physical safeguards which are appropriate to the size and complexity of Avalon's operations, the nature and scope of Avalon's activities and the sensitivity of the PI that Avalon maintains or otherwise possesses;

(ii) Designated Individual: Avalon shall designate a qualified employee responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials, background and experience in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, and monitoring the Information Security Program. The designated individual shall report regularly to Avalon's Board of Directors, no less than quarterly, on the Information Security Program, Avalon's security posture, and the security risks faced by Avalon;

(iii) Resources: Sufficient resources and support to reasonably ensure the functionality of the Information Security Program as required by this Assurance;

(iv) Monitoring & Logging: Policies and procedures designed to properly log and monitor Avalon's Network. At a minimum: (1) Avalon shall employ tools to log and monitor network traffic to detect and respond to Data Security Incidents; (2) Avalon shall take reasonable steps to properly configure, and regularly update or maintain the tools used pursuant to subsection (1) and log system activity to identify potential Data Security Incidents; and (3) Avalon shall use the tools pursuant to subsection (1) to actively review and analyze the logs of system activity and take appropriate responsive action with respect to any Data Security Incidents;

(v) Network Access/Authentication: Appropriate measures to restrict all personnel access to that which is necessary within Avalon's Network. Avalon shall ensure that all personnel accounts have unique passwords or other appropriate controls across the environment and Multi-Factor Authentication for remotely connecting to the Network. Appropriate measures also include the review and, as appropriate, restriction or disabling of unnecessary accounts on Avalon's Network;

(vi) Email Filtering: Maintain email protection and filtering solutions for all Avalon email accounts, including phishing attacks, SPAM, and anti-malware or reasonably equivalent technology;

(vii) Training—All Personnel: Conduct an initial training for all new employees and, on at least a twice-yearly basis, train existing employees concerning Avalon's information security program, including the proper handling and protection of PI and PHI. At a minimum training shall: (i) cover social engineering schemes, such as phishing email attacks, and include what to do if an employee receives an email attachment from an outside source; (ii) include mock phishing exercises and all employees who fail must successfully complete additional training; and (iii) incorporate a defined process for employees to report any concern about Avalon's security systems, including the process for review of a concern, Avalon's response to the concern, and whether and when the individual designated under paragraph 21(b)(ii) was informed of the concern. Avalon shall provide the training required under this paragraph to all employees within thirty (30) days of the Effective Date or within thirty (30) days of employment; and

(viii) Training—Information Security Personnel: Employees who are responsible for implementing, maintaining, or monitoring the Information Security Program ("InfoSec Personnel") shall receive and continue to receive specialized training on safeguarding and protecting PI. Avalon shall provide the training required under this paragraph to all current InfoSec Personnel within forty-five (45) days of the Effective Date or within sixty (60) days of an employee becoming InfoSec Personnel.

(c) **Risk Assessment Program.** Avalon shall develop, implement and maintain a risk assessment program to identify, address, and, as appropriate, remediate risks affecting its Covered Systems. Avalon is permitted to simultaneously satisfy this requirement and the requirement for a HIPAA Security Risk Assessment as set out in section 21(f)(ii). Avalon shall maintain all assessment and testing reports required under this paragraph for a period of not less than seven (7) years, and make them available to the Attorneys General's offices within fourteen (14) days of request. At a minimum, Avalon's risk assessment program shall include:

(i) Biannual Risk Assessment: Performance of an internal risk assessment twice per year that includes, at a minimum, an assessment of all reasonably anticipated, internal and external risks to the security, confidentially, or availability of PI and PHI collected, processed, transmitted, stored, or disposed of by Avalon;

(ii) Penetration Testing: Establishment of a risk-based penetration testing program reasonably designed to regularly identify, assess and remediate penetration vulnerabilities within Avalon's computer network, which shall include annual external penetration tests or a reasonably equivalent technology and appropriate remediation of vulnerabilities reveled by such testing; and

(iii) Annual Third Party Assessment: Obtaining an information security risk assessment and report from an independent third party ("Third Party Assessor"), using procedures and standards generally accepted in the profession, annually for a period of seven (7) years following Avalon's execution of this Assurance. The initial assessment required under this paragraph shall be completed within one-hundred eighty (180) days of the Effective Date. For all future assessments, the internal risk assessments and penetration testing reports required by paragraphs 21(c)(i) – (ii) shall be made available for inspection by the Third Party Assessor.

(d) **Email Data Retention.** Avalon shall permanently delete emails containing PI and PHI as soon as there is no legal or business purpose to retain the emails.

(e) **Email Encryption**. Avalon shall implement email encryption standards for all email transmissions containing PHI. Avalon employees shall not use email for permanent storage of PHI. Avalon employees should only record patient treatment information in patient record systems.

(f) **HIPAA Compliance**. Avalon shall develop, implement and maintain a comprehensive information security program sufficient to protect against reasonably anticipated threats to the security of electronic PHI in compliance with HIPAA Security Rules ("HIPAA

Information Security Program"). This HIPAA Information Security Program is permitted to simultaneously comply with this section and section 21(b). These measures shall include:

(i) Designated Individual: Designation of a HIPAA Compliance Officer responsible for the administration of all HIPAA compliance actions with the credentials, background and understanding of HIPAA appropriate to the level, size, and complexity of their role as the HIPAA Compliance Officer;

(ii) Risk Analysis: An accurate and thorough enterprise-wide analysis of security risks and vulnerabilities that incorporate all data systems, programs, and applications owned, controlled, or managed by Avalon that contain, store, transmit, or receive electronic PHI consistent with 45 C.F.R. § 164.308(a)(1)(ii)(A) within sixty (60) days of the Effective Date;

(iii) Policies & Procedures: A review and revision, as reasonably necessary, of Avalon's current policies and procedures regarding: (i) technical access controls for network or server equipment and systems to ensure authorized access is limited to the minimum amount necessary to prevent impermissible access and disclosure of electronic PHI in compliance with 45 C.F.R. § 164.312(a); (ii) information system activity review for the regular review of audit logs, access reports, and Data Security Incident tracking reports to monitor and respond to suspicious events pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(D); (iii) technical safeguards to examine the activity in systems that contain electronic PHI pursuant to 45 C.F.R. § 164.312(b); and (iv) incident response and reporting to identify and respond to a known Data Security Incident, and document the incident and outcome pursuant to 45 C.F.R. § 164.308(a)(6)(ii) within sixty (60) days of the Effective Date; and

(iv) Monitoring: A written plan to monitor compliance with paragraph 21(f). The plan shall, at a minimum, (i) require the HIPAA Compliance Officer to report regularly to Avalon's Board of Directors, no less than quarterly, on Avalon's compliance

with HIPAA Security Rules and the security risks to PHI maintained by Avalon, (ii) implement a comprehensive audit protocol for system activity review, and (iii) create documentation requirements for any found risks and steps taken to mitigate these risks. Avalon shall maintain the plan for a period of seven (7) years and make the plan available to the Attorneys General offices within fourteen (14) days of request.

21. Avalon may satisfy paragraphs 20 and 21 above through the review, maintenance and, if necessary, updating of existing policies, procedures, and plans.

22. Upon execution of this Assurance, Avalon shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program or HIPAA Information Security Program.

PAYMENT TO STATE

23. Avalon shall pay a total sum of $200,000.00 to the Attorneys General. Said payment shall be divided and paid by Avalon directly to each of the Attorneys General in an amount to be designated by the Attorneys General and communicated to Avalon, along with instructions for such payments. Payment shall be made in full within thirty (30) business days of the Effective Date and receipt of payment instructions by Avalon, except that where state law requires judicial or other approval of the Assurance, payment shall be made no later than thirty (30) days after notice from the relevant Attorney General that such final approval for the Assurance has been secured.

24. Of the total amount, Avalon shall pay $100,000.00 to the Utah Attorney General. The payment shall be used for purposes that may include, but are not limited to, attorneys' fees, and other costs of investigation and litigation, or may be placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education or redress, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, and/or for other uses permitted by state law, at the sole discretion of the Utah Attorney General.

ADDITIONAL PROVISIONS

25. Avalon will create and maintain for a period of at least seven (7) years from the entry date of this Assurance all records necessary to demonstrate Avalon's compliance with its assurances stated herein. Avalon will provide such records to the Attorneys General within fourteen (14) days of its request.

26. Within thirty (30) days of the Effective Date, Avalon will deliver a copy of this Assurance to its current officers and Board of Directors. In the event that any person assumes the role of officer or becomes a member of the Board of Directors and such person has not been previously delivered a copy of this Assurance, Avalon shall deliver a copy of this Assurance to such person within thirty (30) days from the date such person assumes their position and maintain a record of such.

27. The parties acknowledge that they have not entered into any other promises, representations, or agreements of any nature. The parties further acknowledge that this Assurance constitutes a single and entire agreement that is not severable or divisible, except if any provision herein is found to be legally insufficient or unenforceable, the remaining provisions shall continue in full force and effect.

28. Under no circumstances shall this Assurance or the name of the Attorneys General or the offices of the Attorneys General, or any of its employees or representatives, be used by Avalon or by its officers, employees, representatives, or agents in conjunction with any business activity of Avalon.

29. This Assurance is binding on Avalon and its owners, directors, successors, assignees, transferees, officers, agents, partners, employees, representatives, and all other persons acting in concert or participating with Avalon in the context of conducting Avalon's business.

NOTICE

30. Any notices or other documents to be provided to the Parties pursuant to the Assurance shall be sent to the following address via first class and electronic mail, unless a different address is specified in writing by the party changing such address:

For the Attorney General: State of Utah

Tara Pincock, Assistant Attorney General, Antitrust Section

Utah Office of Attorney General

160 E 300 S, 5th Floor

P.O. Box 140874

Salt Lake City, Utah 84114

tpincock@agutah.gov

For Avalon:

Lindsay B. Nickle

Lewis Brisbois Bisgaard and Smith, LLP

2100 Ross Avenue, Suite 2000

Dallas, Texas 75243

Phone: 806.535.0274

Email: Lindsay.nickle@lewisbrisbois.com

APPROVED:
ATTORNEY GENERAL, FOR THE STATE OF UTAH AND ON BEHALF OF THE UTAH DIVISION OF CONSUMER PROTECTION

Sean D. Reyes,
Utah Attorney General

By: Tara W. Pincock Date: December 22, 2022

Tara W. Pincock
Assistant Attorney General
Office of the Attorney General of Utah
160 East 300 South, 5th Floor
P.O. Box 140874
Salt Lake City, UT 84114-0874
tpincock@agutah.gov

[Additional approvals on subsequent pages]

APPROVED:

AVALON HEALTHCARE MANAGEMENT, INC.

By:  Date: 12-5-22

Anne H. Stuart
EVP and Chief Financial Officer
Avalon Health Care Management, Inc.
206 North 2100 West
Salt Lake City, UT 84116
Phone: 801.325.0179
Email: Anne.Stuart@AvalonHealthcare.com