

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

IN THE CIRCUIT COURT OF THE STATE OF OREGON
FOR THE COUNTY OF MULTNOMAH

IN THE MATTER OF: AVALON HEALTHCARE MANAGEMENT, INC., Respondent,	Case No. ASSURANCE OF VOLUNTARY COMPLIANCE
--	--

1.

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.

INTRODUCTION

2.

This Assurance resolves the State of Oregon’s concerns that Avalon violated the Oregon Unlawful Trade Practices Act, ORS 646.605 – ORS 646.656 (the “Consumer Protection Act”).

3.

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

///

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

4.

Avalon is a Utah corporation with care facilities located in Oregon.

PROCEDURE

5.

This Assurance is a settlement of a disputed matter and an agreement between Avalon and the Oregon Attorney General acting pursuant to ORS 646.632.

6.

Avalon waives receipt of notice from the Oregon Attorney General pursuant to ORS 646.632(2) of the alleged unlawful trade practice and relief to be sought.

7.

Avalon understands and agrees that this Assurance will be submitted to the Circuit Court of the State of Oregon for Multnomah County for approval, and, if approved will be filed with the court pursuant to ORS 646.632.

8.

Avalon waives any further notice of submission to and filing with the court of this Assurance.

9.

Avalon understand that, in addition to any other sanctions which may be imposed under this Assurance, the Oregon Attorney General reserves all statutory and legal remedies for violation of the terms of this Assurance pursuant to ORS 646.632(4) and ORS 646.642.

DEFINITIONS

10.

“Consumer” shall mean an individual resident of the Attorneys General’s states.

11.

“Consumer Protection Laws” shall mean ORS 646.605 et seq., and Utah Code § 13-44-201.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

12.

“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.

13.

“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.

14.

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

15.

“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.

16.

“Effective Date” shall be immediately upon execution by Avalon of this Assurance.

17.

“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.

18.

“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

1 Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department
2 of Health and Human Services (“HHS”) Regulations, 45 C.F.R. §§ 160 et seq.

3 19.

4 “Multi-Factor Authentication” means authentication through verification of at least two
5 of the following authentication factors: (i) knowledge factors, such as a password, (ii) possession
6 factors, such as a token, connection through a known authenticate source, or a text message on a
7 mobile phone, or (iii) inherent factors, such as biometric characteristics.

8 20.

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

12 21.

13 “Personal Information” or “PI” shall mean the data elements in the definitions found in ORS
14 646A.06 and Utah Code § 13-44-102.

15 22.

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

18 23.

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

23 **ASSURANCES**

24 24.

25 Avalon shall comply with the Consumer Protection Laws and HIPAA by adopting
26 reasonable data security practices to adequately protect the security, confidentiality, and integrity

1 of all PI and PHI which Avalon collects, uses, and maintains, as well as by complying with the
2 reporting and notification requirements set forth in the Data Breach Notification Laws.

3 25.

4 Avalon agrees to adhere to each of the following requirements:

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

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

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

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

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

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

23 (b) **Information Security Program.** Within sixty (60) days of the Effective Date,
24 Avalon shall develop, implement, and maintain a comprehensive written information security
25 program ("Information Security Program") that includes at least the security requirements set
26 forth in paragraph 25(b)(i) – (viii) of this assurance. Avalon shall review the Information

1 Security Plan not less than annually and make any updates necessary to ensure the reasonable
2 protection of the security, integrity, and confidentiality of PI and PHI that Avalon collects,
3 stores, transmits, and maintains. The Information Security Program is permitted to
4 simultaneously comply with this section and section 25(f) addressing HIPAA compliance.

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

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

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

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

1 respect to any Data Security Incidents;

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

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

11 (vii) Training—All Personnel: Conduct an initial training for all new
12 employees and, on at least a twice-yearly basis, train existing employees concerning
13 Avalon’s information security program, including the proper handling and protection of
14 PI and PHI. At a minimum training shall: (i) cover social engineering schemes, such as
15 phishing email attacks, and include what to do if an employee receives an email
16 attachment from an outside source; (ii) include mock phishing exercises and all
17 employees who fail must successfully complete additional training; and (iii) incorporate a
18 defined process for employees to report any concern about Avalon’s security systems,
19 including the process for review of a concern, Avalon’s response to the concern, and
20 whether and when the individual designated under paragraph 25(b)(ii) was informed of
21 the concern. Avalon shall provide the training required under this paragraph to all
22 employees within thirty (30) days of the Effective Date or within thirty (30) days of
23 employment; and

24 (viii) Training—Information Security Personnel: Employees who are
25 responsible for implementing, maintaining, or monitoring the Information Security
26 Program (“InfoSec Personnel”) shall receive and continue to receive specialized training

1 on safeguarding and protecting PI. Avalon shall provide the training required under this
2 paragraph to all current InfoSec Personnel within forty-five (45) days of the Effective
3 Date or within sixty (60) days of an employee becoming InfoSec Personnel.

4 (c) **Risk Assessment Program.** Avalon shall develop, implement and maintain a risk
5 assessment program to identify, address, and, as appropriate, remediate risks affecting its
6 Covered Systems. Avalon is permitted to simultaneously satisfy this requirement and the
7 requirement for a HIPAA Security Risk Assessment as set out in section 25(f)(ii). Avalon shall
8 maintain all assessment and testing reports required under this paragraph for a period of not less
9 than seven (7) years, and make them available to the Attorneys General’s offices within fourteen
10 (14) days of request. At a minimum, Avalon’s risk assessment program shall include:

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

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

20 (iii) Annual Third Party Assessment: Obtaining an information security risk
21 assessment and report from an independent third party (“Third Party Assessor”), using
22 procedures and standards generally accepted in the profession, annually for a period of
23 seven (7) years following Avalon’s execution of this Assurance. The initial assessment
24 required under this paragraph shall be completed within one-hundred eighty (180) days of
25 the Effective Date. For all future assessments, the internal risk assessments and

26 ///

1 penetration testing reports required by paragraphs 25(c)(i) – (ii) shall be made available
2 for inspection by the Third Party Assessor.

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

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

9 (f) **HIPAA Compliance.** Avalon shall develop, implement and maintain a
10 comprehensive information security program sufficient to protect against reasonably anticipated
11 threats to the security of electronic PHI in compliance with HIPAA Security Rules (“HIPAA
12 Information Security Program”). This HIPAA Information Security Program is permitted to
13 simultaneously comply with this section and section 25(b). These measures shall include:

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

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

23 (iii) Policies & Procedures: A review and revision, as reasonably necessary, of
24 Avalon’s current policies and procedures regarding: (i) technical access controls for
25 network or server equipment and systems to ensure authorized access is limited to the
26 minimum amount necessary to prevent impermissible access and disclosure of electronic

1 PHI in compliance with 45 C.F.R. § 164.312(a); (ii) information system activity review
2 for the regular review of audit logs, access reports, and Data Security Incident tracking
3 reports to monitor and respond to suspicious events pursuant to 45 C.F.R.
4 § 164.308(a)(1)(ii)(D); (iii) technical safeguards to examine the activity in systems that
5 contain electronic PHI pursuant to 45 C.F.R. § 164.312(b); and (iv) incident response and
6 reporting to identify and respond to a known Data Security Incident, and document the
7 incident and outcome pursuant to 45 C.F.R. § 164.308(a)(6)(ii) within sixty (60) days of
8 the Effective Date; and

9 (iv) Monitoring: A written plan to monitor compliance with paragraph 25(f).
10 The plan shall, at a minimum, (i) require the HIPAA Compliance Officer to report
11 regularly to Avalon’s Board of Directors, no less than quarterly, on Avalon’s compliance
12 with HIPAA Security Rules and the security risks to PHI maintained by Avalon, (ii)
13 implement a comprehensive audit protocol for system activity review, and (iii) create
14 documentation requirements for any found risks and steps taken to mitigate these risks.
15 Avalon shall maintain the plan for a period of seven (7) years and make the plan available
16 to the Attorneys General offices within fourteen (14) days of request.

17 26.

18 Avalon may satisfy paragraphs 24 and 25 above through the review, maintenance and, if
19 necessary, updating of existing policies, procedures, and plans.

20 27.

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

24 ///

25 ///

26 ///

1 **PAYMENT TO STATE**

2 28.

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

11 29.

12 Of that total amount, Avalon shall pay to the Oregon Attorney General ONE HUNDRED
13 THOUSAND DOLLARS (\$100,000.00). The payment shall be used by the Oregon Attorney
14 General for purposes that may include, but are not limited to, attorneys’ fees, and other costs of
15 investigation and litigation, or may be placed in, or applied to, any consumer protection law
16 enforcement fund, including future consumer protection or privacy enforcement, consumer
17 education or redress, litigation or local consumer aid fund or revolving fund, used to defray the
18 costs of the inquiry leading hereto, and/or for other uses permitted by state law, at the sole
19 discretion of the Oregon Attorney General.

20 **ADDITIONAL PROVISIONS**

21 30.

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

26 ///

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

31.

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.

32.

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.

33.

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.

34.

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.

///
///
///
///

1 **NOTICE**

2 35.

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

6 For the Attorney General:

7 Kristen G. Hilton
8 Assistant Attorney General
9 Oregon Department of Justice
10 Of Attorneys for Plaintiff
11 Consumer Protection Section
12 100 SW Market Street
13 Portland, OR 97201
14 Phone: 503-931-5790
15 Email: kristen.hilton@doj.state.or.us

12 For Avalon:

13 Lindsay B. Nickle
14 Lewis Brisbois Bisgaard and Smith, LLP
15 2100 Ross Avenue, Suite 2000
16 Dallas, Texas 75243
17 Phone: 806.535.0274
18 Email: Lindsay.nickle@lewisbrisbois.com

17 **APPROVAL BY COURT**

18 APPROVED for filing and so ORDERED:

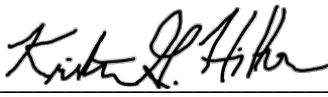
19
20
21
22
23
24 Submitted by: Kristen G. Hilton, OSB#151950
25 Assistant Attorney General
26 Attorney for State of Oregon

26 [Additional approvals on subsequent pages]

1 APPROVED:
2 ELLEN F. ROSENBLUM
3 ATTORNEY GENERAL, THE STATE OF OREGON

4

5

6 By: 

Date: 12/22/22

7

KRISTEN G. HILTON, OSB#151950
Assistant Attorney General
Oregon Department of Justice
Of Attorneys for Plaintiff
Consumer Protection Section
100 SW Market Street
Portland, OR 97201
Phone: 503-931-5790
Email: kristen.hilton@doj.state.or.us

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

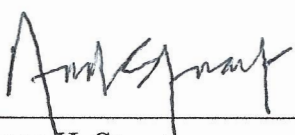
24

25

26

1 APPROVED:


2 AVALON HEALTHCARE MANAGEMENT, INC.

3
4 By: 

Date: 12-5-22

5 Anne H. Stuart
6 EVP and Chief Financial Officer
7 Avalon Health Care Management, Inc.
8 206 North 2100 West
9 Salt Lake City, UT 84116
10 Phone: 801.325.0179
11 Email: Anne.Stuart@AvalonHealthcare.com

10 COUNSEL FOR AVALON HEALTHCARE MANAGEMENT, INC.

11
12 By: 

Date: 12/5/2022

13 Lindsay B. Nickle, TBN 24007747
14 Lewis Brisbois Bisgaard and Smith, LLP
15 2100 Ross Avenue, Suite 2000
16 Dallas, Texas 75243
17 Phone: 806.535.0274
18 Email: Lindsay.nickle@lewisbrisbois.com

1
2 **CERTIFICATE OF READINESS**

3 This proposed **Assurance of Voluntary Compliance** is ready for judicial signature because:

- 4 1. [X] Each opposing party affected by this order has stipulated to the order, as shown
5 by each opposing party's signature on the document being submitted.
6 2. [] Each opposing party affected by this order has approved the order, as shown by
7 signature on the document being submitted or by written confirmation of approval
8 sent to me.
9 3. [] I have served a copy of this order on all parties entitled to service and provided
10 written notice of the objection period, and:
11 a. [] No objection has been served on me within that time frame.
12 b. [] I received objections that I could not resolve with the opposing party
13 despite reasonable efforts to do so. I have filed with the court a copy of the
14 objections I received and indicated which objections remain unresolved.
15 c. [] After conferring about objections, [*role and name of opposing party*]
16 agreed to file any remaining objection with the court by [*date*], which
17 predated my submission.
18 4. [] The relief sought is against an opposing party who has been found in default.
19 5. [] An order of default is being requested with this proposed judgment.
20 6. [] Service is not required by statute, rule, or otherwise.

21 Dated December 22th, 2022.



22 KRISTEN G. HILTON, OSB#151950
23 Assistant Attorney General
24 Civil Enforcement Division
25 Oregon Department of Justice
26 100 Market Street
Portland, OR 97201
Phone: (971) 673-1880
Fax: (971) 673-1888
Email: Kristen.Hilton@doj.state.or.us