Many organizations are now using telehealth to deliver counseling and consultation services. There are many platforms which can enable HIPAA-compliant telehealth sessions. One of these is Zoom.

We like Zoom because it is economical and widely-used, so clients are less likely to have to get accustomed to the platform. Any organizational decision to use telehealth, however, should be considered carefully and evaluated for legal, security and compliance risks. The following "Business Associate Agreement" was downloaded 8/26/2021 from zoom.us/healthcare and illustrates the standard agreement of Zoom (as of the date of download) with regard to users of its Healthcare solution for videoconferencing. Regardless of telehealth platform, we encourage potential telehealth users to review and ensure they understand this type of agreement before commencing telehealth services.

More information is also available here: https://support.zoom.us/hc/en-us/articles/207652183-HIPAA-Business-Associate-Agreement-BAA-

Zoom Video Communications, Inc.

BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT ("**Agreement**" or "**BAA**") is made as of today between **Zoom Video Communications Inc**. and Affiliates, located at 55 Almaden Blvd, Suite 600, San Jose, CA 95113, hereinafter referred to as "**Zoom**" or "**Business Associate**", and the account owner, located at the account owner's address on file , hereinafter referred to as "**Company**" or "**Customer**".

This BAA forms part of the Master Subscription Agreement, Terms of Service, Terms of Use, or any other agreement pertaining to the delivery of services (the "**Agreement**") between Zoom and the Customer named in such Agreement to reflect the parties' agreement with regard to the Processing of Protected Health Information (as defined below). Zoom's liability arising out of or related to this BAA will be determined solely in accordance with the parties' Agreement.

RECITALS

Company is a HIPAA Covered Entity or Business Associate and Zoom is acting as a service provider to Company and may receive, use, maintain, disclose or otherwise process Protected Health Information for or on behalf of Company.

The parties desire to comply with relevant Federal and State confidentiality standards, including but not limited to: the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"); 45 CFR part 160 and part 164, subparts A and E (the "**Privacy Rule**"); 45 C.F.R. Part 160 and

Subparts A and C of Part 164 (the "**Security Rule**"), and The Health Information Technology for Economic and Clinical Health Act (the "**HITECH Act**").

NOW THEREFORE, the parties to this Agreement hereby agree as follows:

1. Definitions. Terms used, but not otherwise defined, in this Agreement shall have the meaning ascribed to them by HIPAA, the Privacy Rule, the Security Rule, and/or the HITECH Act.

a. **Affiliate** means, with respect to a party, any entity that directly or indirectly controls, is controlled by or is under common control with that party. For purposes of this Agreement, "control" means an economic or voting interest of at least fifty percent (50%) or, in the absence of such economic or voting interest, the power to direct or cause the direction of the management and set the policies of such entity.

b. **Breach** shall mean any acquisition, access, use, or disclosure of Unsecured Protected Health Information that is inconsistent with the terms of this BAA and that compromises the security or privacy of the Unsecured Protected Health Information. Whether an acquisition, access, use, or disclosure of Unsecured Protected Health Information compromises its security or privacy shall be determined by reference to the definition of "breach" in 45 C.F.R. § 164.402.

c. **Business Associate** shall have the meaning specified in 45 CFR § 160.103.

d. **Covered Entity** shall have the meaning specified in 45 C.F.R. § 160.103.

e. **Electronic PHI** is any PHI that is transmitted by or maintained in electronic media.

f. **Protected Health Information or PHI** shall have the same meaning as the term "protected health information" in 45 CFR § 160.103 of HIPAA, provided that it is limited to such protected health information that is received by Zoom from, or created, received, maintained, or transmitted by Zoom on behalf of, Customer through Customer's use of the Services pursuant to this Agreement.

g. **Required by law** shall mean a mandate contained in law that compels a use or disclosure of Protected Health Information.

h. **Secretary** shall mean the Secretary of the Department of Health and Human Services and those employees or agents designated to act on the Secretary's behalf.

i. **Security or Security Measures** means the administrative, physical, and technical safeguards and documentation requirements specified in the Security Rule.

j. **Service Agreement** shall mean the agreement(s) and Terms of Service pursuant to which Zoom is to provide video communication services and other related services to Covered Entity.

k. **Unsecured Protected Health Information** is any Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary.

2. Permitted Uses and Disclosures of Protected Health Information.

a. **Performance of the Agreement for Zoom Services**. Zoom agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement, as required or permitted by the Service Agreement, or as required or permitted by law, provided such use or disclosure would not violate HIPAA if done by Customer, unless expressly permitted under this Agreement.

b. **Management, Administration, and Legal Responsibilities**. Except as otherwise limited in this BAA, Zoom may Use and Disclose Protected Health Information for the proper management and administration of Zoom and/or to carry out the legal responsibilities of Zoom, provided that any Disclosure may occur only if: (1) Required by law; or (2) Zoom obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by law or for the purpose for which it was Disclosed to the person, and the person notifies Zoom of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.

3. Parties Responsibilities with Respect to Protected Health Information.

a. **Zoom's Responsibilities.** To the extent Zoom is acting as a Business Associate, Zoom agrees to the following:

i. *Limitations on Use and Disclosure.* Zoom shall not Use and/or Disclose the Protected Health Information except as otherwise limited in this Agreement or by application of 42 C.F.R. Part 2 with respect to Part 2 Patient Identifying Information, for the proper management and administration of Zoom or to carry out the legal responsibilities of Zoom; provided that in doing so, Zoom will only use the minimum necessary Protected Health information necessary for the proper management and administration of Zoom's business specific purposes, or to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1) and, where applicable, 42 C.F.R. Part 2.

ii. *Safeguards.* Zoom shall: (1) use reasonable and appropriate safeguards to prevent inappropriate Use and Disclosure of Protected Health Information other than as provided for in this BAA; and (2) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule.

iii. *Subcontractors*. Notwithstanding anything to the contrary in the Services Agreement, Business Associate, subject to the restrictions set forth in this provision, may use subcontractors to fulfill its obligations under this BAA. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Zoom shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Zoom to agree in writing to: (1) the same or more stringent restrictions and conditions that apply to Zoom with respect to such Protected Health Information; (2) appropriately safeguard the Protected Health Information; and (3) comply with the applicable requirements of 45 CFR Part 164 Subpart C of the Security Rule. Zoom remains responsible for its Subcontractors' compliance with obligations in this BAA.

iv. *Reporting.* Zoom shall report to Customer: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which Zoom becomes aware; (2) any Security Incident of which it becomes aware, provided that notice is hereby deemed given for Unsuccessful Security Incidents (as defined below) and no further notice of such Unsuccessful Security Incidents shall be given; and/or (3) any Breach of Customer's Unsecured Protected Health Information that Zoom may discover (in accordance with 45 CFR § 164.410 of the Breach Notification Rule). Notification of a Breach will be made without unreasonable delay, but in no event more than ten (10) business days after Zoom's discovery of a Breach. Notification of a Successful Security Incident or other impermissible Use and/or Disclosure of Protected Health Information by Zoom or its subcontractors will be made without unreasonable delay, but in no event more than twenty (20) business days after Zoom's discovery thereof.

For purposes of this Section, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on Zoom's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information. Notification(s) under this Section, if any, will be delivered to contacts identified by Customer pursuant to Section 3b(ii) (Contact Information for Notices) of this BAA. Zoom's obligation to report under this Section is not and will not be construed as an acknowledgement by Zoom of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

v. *Disclosures to the Secretary*. Zoom agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or received by Zoom on behalf of, Customer available to the Customer, or at the request of the Customer to the Secretary, in a time and manner designated by the Customer or the Secretary, for purposes of the Secretary determining Customer's compliance with the Privacy Rule.

vi. *Access.* Zoom agrees to provide access, at the request of Customer and in the time and manner designated by Customer, to Protected Health Information in a Designated Record Set to Customer or, as directed by Customer, to an Individual (as defined in 45 C.F.R. § 160.103) in order to meet the requirements under 45 CFR §164.524, provided that nothing in this section shall require Business Associate to retain or obtain access to Protected Health Information not already being retained or accessed by Business Associate pursuant to the terms of this agreement.

vii. *Amendment.* Zoom agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Customer directs or agrees to pursuant to 45 CFR §164.526 at the request of Customer or an Individual, and in the time and manner designated as reasonably requested by Customer, provided that nothing in this section shall require Business Associate to retain or obtain access to Protected Health Information not already being retained or accessed by Business Associate pursuant to the terms of this BAA and that nothing in this section shall require Business Associate to assign a Designated Record set where not reasonably practicable in light of Zoom's encryption practices.

viii. *Accounting of Disclosures.* Zoom, at the request of Customer, shall make available to Customer, and in the time and manner designated as reasonably requested by Customer, such information relating to Disclosures made by Zoom as required for Customer to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.

ix. *Performance of a Covered Entity's Obligations.* To the extent Zoom is to carry out a Covered Entity obligation under the Privacy Rule, Zoom shall comply with the requirements of the Privacy Rule that apply to Customer in the performance of such obligation.

b. Customer's Responsibilities

i. *No Impermissible Requests.* Customer shall not request Zoom to Use or Disclose Protected Health Information in any manner that would not be

permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).

ii. *Contact Information for Notices.* Customer hereby agrees that any reports, notification, or other notice by Zoom pursuant to this BAA may be made electronically to the Customer contact specified in Section 7 (Notices) below. Customer shall ensure that such contact information remains up to date during the term of this BAA. Failure to submit and maintain as current the aforementioned contact information may delay Zoom's ability to provide Breach notification under this BAA.

iii. *Safeguards and Appropriate Use of Protected Health Information.* Customer is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation. It is Customer's obligation to exclude Protected Health Information from information Customer submits to technical support personnel through a technical support request. Customer is solely responsible for ensuring the Protected Health Information it transmits via Zoom may be legally disclosed to the communications recipient(s).

iv. *Communicating Changes to Zoom*. Customer shall notify Zoom of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Zoom's use or disclosure of Protected Health Information.

v. *Communicating Restrictions to Zoom.* Customer shall notify Zoom of any restriction to the use or disclosure of Protected Health Information that Customer has agreed to in accordance with 45 CFR §164.522 or 42 C.F.R. Part 2, to the extent that such restriction may affect Zoom's use or disclosure of Protected Health Information.

vi. *Communicating Restrictions in Notices of Privacy Practices to Zoom*. Customer shall notify Zoom of any limitation(s) in any applicable notice of privacy practices in accordance with 45 CFR Section 164.520, to the extent that such limitation may affect Zoom's use or disclosure of Protected Health Information.

4. Term and Termination.

a. **Term.** The term of this Agreement shall begin as of the effective date of the Service Agreement or when Customer introduces Protected Health Information to the Service environment and shall terminate when all of the Protected Health Information provided by Customer to Zoom, or created or received by Zoom on behalf of Customer, is destroyed or returned to Customer, or, if it is infeasible to

return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

b. **Termination for Breach.** Upon Customer's knowledge of a material breach by Zoom, Customer shall either:

i. Provide an opportunity for Zoom to cure the breach or end the violation and terminate this Agreement and the Service Agreement if Zoom does not cure the breach or end the violation within a reasonable time specified by Customer;

ii. Immediately terminate this Agreement and the Service Agreement if Zoom has breached a material term of this Agreement and cure is not possible; or

iii. If neither termination nor cure is feasible, Customer shall report the violation to the Secretary.

c. **Return, Destruction, or Retention of Protected Health Information Upon Termination.** Except as provided in paragraph (d) of this Section, upon any termination or expiration of this Agreement, Zoom shall return or destroy all Protected Health Information received from Customer, or created or received by Zoom on behalf of Customer. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Zoom. Zoom shall retain no copies of the Protected Health Information. Notwithstanding the foregoing, Business Associate may retain a copy of PHI received from, or created or received by Business Associate for or on behalf of Covered Entity which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities, provided that Business Associate extends the protections of this Agreement to such information.

d. In the event that Zoom determines that returning or destroying the Protected Health Information is infeasible, Zoom shall provide to Customer notification of the conditions that make return or destruction infeasible. Upon Customer's written agreement that return or destruction of Protected Health Information is infeasible, Zoom shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Zoom maintains such Protected Health Information.

5. Notices.

Any notices to be given under this Agreement, including without limitation any Breach notification, to a party shall be made in writing and delivered via electronic mail to

the contact at the address indicated below (or at such other address as a party may specify by notice to the others pursuant hereto).

Notices shall be addressed as follows:

If to Zoom, to:

Zoom Video Communications, Inc.

Email: privacy@zoom.us

Attention: Privacy Officer

And to legal@zoom.us

Customer account contact information on file.

6. No Agency Relationship. It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Customer and Zoom under HIPAA or the Privacy Rule, Security Rule, or Breach Notification Rule. No terms or conditions contained in this BAA shall be construed to make or render Zoom an agent of Customer.

7. No Third Party Beneficiary. This Agreement is intended for the sole benefit of the Business Associate and Prime Subcontractor and does not create any third party beneficiary rights.

8. Miscellaneous.

a. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

b. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Customer to comply with the requirements of HIPAA, the Privacy Rule, the Security Rule, the HITECH Act, and 42 C.F.R. Part 2.

c. The respective rights and obligations of Zoom under Section 6(d) and (e) of this Agreement shall survive the termination of this Agreement.

d. Any ambiguity in this Agreement shall be resolved to permit Customer to comply with HIPAA, the Security Rule, any applicable aspects of the Privacy Rule, the HITECH Act, and 42 C.F.R. Part 2.

e. If Zoom knows of a pattern of activity or practice of the Customer that constitutes a material breach or violation of the Customer's obligations under this Agreement, Zoom must take reasonable steps to notify Customer to cure the breach or end the violation. If the steps are unsuccessful, Zoom may terminate this Agreement or, if termination is not feasible, report the problem to the Secretary of DHHS. Zoom shall provide written notice to the Customer of any activity or practice that is believed to constitute a material breach or violation of the Agreement within 5 days of discovery and shall meet with the Customer to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

f. This Agreement constitutes the entire agreement between the parties hereto with respect to the obligations set forth herein and supersedes and replaces any prior agreements between the parties relating to such obligations.

[*signature page follows*]

IN WITNESS WHEREOF, the undersigned have executed this Agreement as of the date first set forth above.

BUSINESS ASSOCIATE:

Account Owner

Zoom Video Communications, Inc.