AWS ORGANIZATIONS BUSINESS ASSOCIATE ADDENDUM

THIS AWS ORGANIZATIONS BUSINESS ASSOCIATE ADDENDUM (this "**Addendum**") is an agreement between Amazon Web Services, Inc. ("**AWS**") and you or the entity you represent ("**you**" or "**your**"), is an addendum to the Master Account Agreement and each applicable Member Account Agreement, as described herein (as applicable, the "**Agreement**"), and is entered into by the Master Entity on behalf of itself and each Member Entity. This Addendum takes effect on the date (the "**Addendum Effective Date**") when the Master Entity clicks the "Accept AWS Business Associate Addendum for this Organization" button (or other electronic means made available by AWS for such purpose) presented with this Addendum (an "**Accept Button**"). You represent to AWS that you are lawfully able to enter into contracts (e.g., you are not a minor). If you are entering into this Addendum for an entity, such as the company you work for, you represent to AWS that you have legal authority to bind that entity.

The parties hereby agree as follows:

1.   Applicability; HIPAA Eligible Services.

1.1. Applicability.

1.1.1.   General. This Addendum applies only to HIPAA Accounts. You acknowledge and agree that this Addendum does not apply to any accounts you may have now or in the future that do not meet all of the requirements of a "HIPAA Account" (as defined in this Addendum), including any accounts that are not joined as Member Accounts in the Organization.

1.1.2.   Applicability to Member Entities. For purposes of this Addendum, with respect to each Member Account, the applicable Member Entity will be deemed to have entered into a separate AWS Business Associate Addendum with AWS under the same terms and conditions as this Addendum (other than the terms of this Addendum that expressly apply only to the Master Entity), and for purposes of this separate AWS Business Associate Addendum between each Member Entity and AWS (a) all references to "you" or "your" in this Addendum will be construed to mean the applicable Member Entity, and (b) all references to the "Agreement" will be construed to mean the applicable Member Account Agreement. The Master Entity represents and warrants that it has and will maintain the full power and authority (i) to enter into this Addendum on behalf of all Member Entities and to legally bind each Member Entity to the terms of this Addendum, and (ii) to terminate this Addendum on behalf of each Member Entity. The Master Entity and each Member Entity will be jointly and severally liable under this Addendum and under the separate AWS Business Associate Addendum between AWS and each Member Entity created hereunder. The Master Entity will defend, indemnify and hold harmless AWS, its Affiliates, and their respective employees, officers, directors, and representatives against all Losses arising from or related to any third-party claim that arises from any breach by the Master Entity of the representations and warranties in this Section 1.1.2.

1.2. HIPAA Eligible Services. You may only use HIPAA Eligible Services to create, receive, maintain, or transmit PHI, and you acknowledge that this Addendum does not apply to PHI that is created, received, maintained, or transmitted through any Services that are not HIPAA Eligible Services. AWS may, in its sole discretion, add or remove Services or functionality of any of the Services to or from the HIPAA Eligible Services from time to time. AWS will provide at least 6 months prior notice to you if AWS decides to remove an existing Service or existing functionality of a Service from the HIPAA Eligible Services. AWS will not be obligated to provide Notice under this Section 1.2 if the removal is necessary to address an emergency or threat to the security or integrity of AWS, respond to claims, litigation, or loss of license rights related to third-party intellectual property rights, or comply with the law or requests of a government entity.

2.   Permitted and Required Uses and Disclosures.

2.1.   Service Offerings. AWS may Use or Disclose PHI for or on behalf of you as specified in the Agreement.

2.2.   Administration and Management of AWS. AWS may use and disclose PHI as necessary for the proper management and administration of AWS. Any Disclosures under this section will be made only if AWS obtains reasonable assurances from the recipient of the PHI that (a) the recipient will hold the PHI confidentially and will Use or Disclose the PHI only as required by law or for the purpose for which it was disclosed to the recipient,

and (b) the recipient will notify AWS of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Obligations of AWS.

3.1. AWS Obligations Conditioned on Appropriate Configurations. For any of your accounts other than a HIPAA Account, AWS does not act as a business associate under HIPAA and will have no obligations under this Addendum. If you have additional accounts that need to be covered under an AWS Business Associate Addendum, you must either (i) log in to AWS Artifact (or any successor Service offered by AWS) under each of those other accounts and accept a separate AWS Business Associate Addendum, or (ii) join such account as a member account in the Organization with the Master Account.

3.2. Limit on Uses and Disclosures. AWS will use or disclose PHI only as permitted by this Addendum or as required by law, provided that any such use or disclosure would not violate HIPAA if done by a Covered Entity, unless permitted under HIPAA for a Business Associate.

3.3. Safeguards. AWS will use reasonable and appropriate safeguards to prevent Use or Disclosure of the PHI other than as provided for by this Addendum, consistent with the requirements of Subpart C of 45 C.F.R. Part 164 (with respect to Electronic PHI) as determined by AWS and as reflected in the Agreement.

3.4. Reporting. For all reporting obligations under this Addendum, the parties acknowledge that, (a) because AWS does not know the nature of PHI contained in any of your accounts, it will not be possible for AWS to provide information about the identities of the Individuals who may have been affected, or a description of the type of information that may have been subject to a Security Incident, Impermissible Use or Disclosure, or Breach, and (b) AWS may provide such reporting to the email address associated with the applicable HIPAA Account(s).

3.4.1. Reporting of Impermissible Uses and Disclosures. AWS will report to you any Use or Disclosure of PHI not permitted or required by this Addendum of which AWS becomes aware.

3.4.2. Reporting of Security Incidents. AWS will report to you on no less than a quarterly basis any Security Incidents involving PHI of which AWS becomes aware in which there is a successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System in a manner that risks the confidentiality, integrity, or availability of such information. Notice is hereby deemed provided, and no further notice will be provided, for unsuccessful attempts at such unauthorized access, use, disclosure, modification, or destruction, such as pings and other broadcast attacks on a firewall, denial of service attacks, port scans, unsuccessful login attempts, or interception of encrypted information where the key is not compromised, or any combination of the above.

3.4.3. Reporting of Breaches. AWS will report to you any Breach of your Unsecured PHI that AWS may discover to the extent required by 45 C.F.R. § 164.410. AWS will make such report without unreasonable delay, and in no case later than 60 calendar days after discovery of such Breach.

3.5. Subcontractors. AWS will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of AWS agree to restrictions and conditions at least as stringent as those found in this Addendum, and agree to implement reasonable and appropriate safeguards to protect PHI.

3.6. Access to PHI. AWS will make PHI in a Designated Record Set available to you so that you can comply with 45 C.F.R. § 164.524.

3.7. Amendment to PHI. AWS will make PHI in a Designated Record Set available to you for amendment and incorporate any amendments to the PHI, as may reasonably be requested by you in accordance with 45 C.F.R. § 164.526.

3.8. Accounting of Disclosures. AWS will make available to you the information required to provide an accounting of Disclosures in accordance with 45 C.F.R. § 164.528 of which AWS is aware, if requested by you. Because AWS cannot readily identify which Individuals are identified or what types of PHI are included in Content you or any End User (a) run on the Services, (b) cause to interface with the Services, or (c) upload to the Services under your account or otherwise transfer, process, use or store in connection with your account

("**Customer Content**"), you will be solely responsible for identifying which Individuals, if any, may have been included in Customer Content that AWS has disclosed and for providing a brief description of the PHI disclosed.

3.9. Internal Records. AWS will make its internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services ("**HHS**") for purposes of determining your compliance with HIPAA. Nothing in this section will waive any applicable privilege or protection, including with respect to trade secrets and confidential commercial information.

4.   Your Obligations.

4.1. Identification of HIPAA Accounts. By clicking an Accept Button, you have identified the Master Account and all Member Accounts as accounts that are eligible to be HIPAA Accounts when they meet all of the requirements of a "HIPAA Account" (as defined in this Addendum).

4.2. Appropriate Use of HIPAA Accounts. You are responsible for implementing appropriate privacy and security safeguards in order to protect your PHI in compliance with HIPAA and this Addendum. Without limitation, you will (a) not include protected health information (as defined in 45 C.F.R. § 160.103) in any Services that are not HIPAA Eligible Services, (b) utilize the highest level of audit logging in connection with your use of all HIPAA Eligible Services, and (c) maintain the maximum retention of logs in connection with your use of all HIPAA Eligible Services.

4.3. Appropriate Configurations. You are solely responsible for configuring, and will configure, each of your HIPAA Accounts, as follows:

4.3.1.   Encryption. You must encrypt all PHI stored in or transmitted using the Services in accordance with the Secretary of HHS's Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html, as it may be updated from time to time, and as may be made available on any successor or related site designated by HHS.

4.4. Necessary Consents. You warrant that you have obtained any necessary authorizations, consents, and other permissions that may be required under applicable law prior to placing Customer Content, including without limitation PHI, on the AWS Network.

4.5. Restrictions on Disclosures. You will not agree to any restriction requests or place any restrictions in any notice of privacy practices that would cause AWS to violate this Addendum or any applicable law.

4.6. Compliance with HIPAA. You will not request or cause AWS to make a Use or Disclosure of PHI in a manner that does not comply with HIPAA or this Addendum.

5.   Term and Termination

5.1. Term. The term of this Addendum will commence (a) with respect to the Master Account, on the Addendum Effective Date, and (b) with respect to each Member Account, on the later of (i) the Addendum Effective Date, or (ii) the date that the applicable Member Account is joined as a member account in the Organization. This Addendum will immediately terminate with respect to the Master Account and all Member Accounts upon the earlier of (A) termination of the Master Account Agreement for any reason, or (B) termination of this Addendum by either the Master Entity or by AWS as set forth in Section 5.2 below. In addition, this Addendum will immediately terminate with respect to an individual Member Account, upon the earlier of (1) removal of such Member Account (such that it is no longer joined) as a member account in the Organization, (2) termination of this Addendum by AWS with respect to the applicable Member Entity as set forth in Section 5.2.2 below, or (3) termination of the applicable Member Account Agreement for any reason.

5.2. Termination.

5.2.1.   By the Master Entity. The Master Entity (and only the Master Entity) has the right to terminate this Addendum for any reason upon notice to AWS by logging in to AWS Artifact (or any successor Service offered by AWS) under the Master Account and clicking a "Terminate AWS Business Associate Addendum for this

Organization" button (or other electronic means made available by AWS for such purpose). Such termination by the Master Entity will apply to the Master Account and to all Member Accounts, and as of the date of such termination the Master Account and all Member Accounts will no longer be covered this Addendum.

5.2.2. By AWS. AWS has the right to terminate this Addendum for any reason upon 90 days prior written notice to the Master Entity. In addition, AWS has the right to terminate this Addendum with respect to any individual Member Entity for any reason upon 90 days prior written notice to the Master Entity or to the applicable Member Entity. A material breach of this Addendum will be treated as a material breach of the Master Account Agreement and the applicable Member Account Agreement.

5.3. Effect of Termination. At termination of this Addendum, AWS, if feasible, will return or destroy all PHI that AWS still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of this Addendum to the information and limit further Uses and Disclosures to those purposes that make the return or destruction of the information infeasible. The parties acknowledge that it is not feasible for AWS to destroy or return PHI upon termination of this Addendum. Termination of this Addendum will not terminate any other AWS Business Associate Addendum(s) then in place between you and AWS, and such other AWS Business Associate Addendum(s) will remain in effect until terminated in accordance with their respective terms.

6. No Agency Relationship. As set forth in the Agreement, nothing in this Addendum is intended to make either party an agent of the other. Nothing in this Addendum is intended to confer upon you the right or authority to control AWS's conduct in the course of AWS complying with the Agreement and Addendum.

7. Nondisclosure. You agree that the terms of this Addendum are not publicly known and constitute AWS Confidential Information under the Agreement.

8. Entire Agreement; Conflict. Except as amended by this Addendum, the Agreement will remain in full force and effect. This Addendum, together with the Agreement as amended by this Addendum: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement; and (b) supersedes all prior agreements and understandings (whether oral or written) between the parties with respect to the subject matter hereof, except that this Addendum will not supersede any other account-specific AWS Business Associate Addendum (an "**AWS Account BAA**") that is in place with respect to the Master Account or any Member Account prior to or after the Effective Date of this Addendum; provided that while this Addendum is in effect with respect to the Master Account or any Member Account, it will apply instead of any AWS Account BAA in place with respect the applicable account. If there is a conflict between the Agreement, this Addendum, or any other amendment or addendum to the Agreement or this Addendum, the document later in time will prevail, except that while this Addendum is in effect with respect to the Master Account or any Member Account, it will control over any AWS Account BAA in place with respect to the applicable account. AWS will not be bound by, and specifically objects to, any term, condition or other provision which is different from or in addition to the provisions of this Addendum (whether or not it would materially alter this Addendum) and which is submitted by you in any order, receipt, acceptance, confirmation, correspondence or other document.

9. Modification. From time to time, AWS may modify the terms of the AWS Business Associate Addendum that it offers to its customers, but no modification or amendment of any portion of this Addendum will be effective unless in writing and accepted by you and by AWS, which acceptance may be made electronically through AWS Artifact (or any successor Service offered by AWS) or through other electronic means made available by AWS for such purpose.

10. Definitions. Unless otherwise expressly defined in this Addendum, all capitalized terms in this Addendum will have the meanings set forth in the Agreement or in HIPAA. Defined terms used in this Addendum with initial letters capitalized have the meanings given below:

"**HIPAA**" means the Administrative Simplification Subtitle of the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, and their implementing regulations.

"**HIPAA Account**" means the Master Account and each Member Account, in each case, (a) that uses only the HIPAA Eligible Services (alone or in combination) to store or transmit any "protected health information" as defined in 45 C.F.R § 160.103, and (b) to which the required security configurations specified in the list of HIPAA Eligible Services, if any, and in Section 4.3 of this Addendum are applied.

"**HIPAA Eligible Services**" means only the Services listed at https://aws.amazon.com/compliance/hipaa-eligible-services-reference (and any successor or related locations designated by AWS), subject to any required security configurations applicable to such Services or functionality of such Services described at such location, as may be updated by AWS from time to time.

"**Master Account**" means the account that you used to log in to AWS Artifact (or any successor Service offered by AWS) to accept this Addendum.

"**Master Account Agreement**" means the AWS Customer Agreement available at http://aws.amazon.com/agreement (as updated from time to time) between Master Entity and AWS, or other agreement between Master Entity and AWS governing Master Entity's use of the Service Offerings under the Master Account.

"**Master Entity**" means you as the individual or entity that opened the Master Account and is responsible for use of the Master Account under the Master Account Agreement.

"**Member Account**" means each account that is joined as a member account in the Organization with the Master Account, and includes accounts that are joined as member accounts in the Organization after the Addendum Effective Date.

"**Member Account Agreement**" means the AWS Customer Agreement available at http://aws.amazon.com/agreement (as updated from time to time) between a Member Entity and AWS, or other agreement between a Member Entity and AWS governing the Member Entity's use of the Service Offerings under a Member Account.

"**Member Entity**" means each individual or entity that (before or after the Addendum Effective Date) opens a Member Account and is responsible for use of the Member Account under the applicable Member Account Agreement.

"**Organization**" means the organization of one or more member accounts for which the Master Account is the master account with "all features" (or any successor functionality offered by AWS giving the master account full access to and control over its member accounts) enabled for all member accounts for purposes of AWS Organizations (or any successor Service offered by AWS).

"**PHI**" means "protected health information" as defined in 45 C.F.R. § 160.103 that is received by AWS from or on behalf of you and that is in a HIPAA Account.

[*Remainder of Page Intentionally Left Blank*]