AWS BUSINESS ASSOCIATE ADDENDUM

THIS AWS BUSINESS ASSOCIATE ADDENDUM (this "**Addendum**") to the AWS Customer Agreement available at http://aws.amazon.com/agreement by and between San Mateo County ("**you**") and Amazon Web Services, Inc. or other agreement between you and AWS governing your use of the Services (the "**Agreement**") is made as of June 25, 2019 (the "**Addendum Effective Date**").

The parties hereby agree as follows:

1. Applicability and Definitions. This Addendum applies only to HIPAA Accounts. A "**HIPAA Account**" means an account under the Agreement: (a) that uses only the HIPAA Eligible Services (alone or in combination) to store or transmit any "protected health information" as defined in 45 CFR 160.103, (b) that you have identified as required under Section 4.1 of this Addendum, and (c) to which you have applied the required security configurations specified in the list of HIPAA Eligible Services (defined below), if any, and in Section 4.3 of this Addendum. You acknowledge that this Addendum does not apply to any other accounts you may have now or in the future, and that any of your accounts that do not satisfy all of the HIPAA Account requirements are not subject to this Addendum. 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. "**HIPAA**" means the Administrative Simplification Subtitle of the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations. "**HIPAA Eligible Services**" means only the Services located 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. 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. "**PHI**" means "protected health information" as defined in 45 CFR 160.103 that is received by AWS from or on behalf of you and that is in a HIPAA Account.

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 that are not HIPAA Accounts, AWS does not act as a business associate under HIPAA and will have no obligations under this Addendum.

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, 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.

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. All of your accounts that you intend to be applicable to this Addendum that contain "protected health information" as defined in 45 CFR 160.103 are identified on Exhibit A to 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 CFR 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, all accounts identified under Section 4.1 of this Addendum, 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 on the Addendum Effective Date and will remain in effect with respect to each account that you identify as being subject to this Addendum until the earlier of the termination of the Agreement or notification by you that an account is no longer subject to this Addendum.

5.2. Termination. Either party has the right to terminate this Addendum for any reason upon 90 days prior written notice to the other party. A material breach of this Addendum will be treated as a material breach of the 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.

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. 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.

9. Counterparts and Facsimile Delivery. This Addendum may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties may sign and deliver this Addendum by facsimile transmission.

[Remainder of Page Intentionally Left Blank]

IN WITNESS WHEREOF, the parties have executed this Addendum as of the Addendum Effective Date.

AMAZON WEB SERVICES, INC.:

By: DocuSigned by: Shannon Lowther
8D4BA0F1C6DA41A...

Name: Shannon Lowther

Title: Authorized Representative

Date signed: May 30, 2019

SAN MATEO COUNTY:

By: _____

Name: Sean Thakkar

Title: Deputy Chief Information Officer

Date signed: June 25, 2019

[Signature Page to AWS Business Associate Addendum]

Exhibit A

AWS Accounts

AWS Account ID
639872916246

This Addendum will cover the account(s) listed above. You may update this list of accounts by providing written notice to AWS at aws-hipaa@amazon.com. Any such update will be effective only upon written acknowledgement of receipt by AWS.

You represent and warrant that you are the owner of all account(s) covered by this Addendum.