DocuSign Business Associate Addendum

Version Date: November 17, 2020

This Business Associate Addendum ("**BAA**") is effective as of the last date signed below ("**BAA Effective Date**") and is made part of the agreement between DocuSign, Inc. ("**DocuSign**") and the County of Monterey, a political subdivision of the State of California, on behalf of the Monterey County Health Department ("**Customer**") for the use of the applicable DocuSign Services to which Customer has subscribed to in an Order Form with DocuSign ("**Agreement**"). Any term not otherwise defined herein shall have the meaning specified in the Agreement or in HIPAA (as defined below). In the event of any inconsistency or conflict between the Agreement and this BAA, the terms of this BAA shall control with respect to the applicable DocuSign Services.

1. Definitions

"**Breach**" shall have the same meaning as "breach" as defined in 45 C.F.R. § 164.402; however, the term "Breach" as used in this BAA shall also mean the unlawful or unauthorized access to, Use or Disclosure of a patient's "medical information" as defined under Cal. Civil Code § 56.05(j), for which notification is required pursuant to Cal. Health & Safety Code 1280.15, or a "breach of the security of the system" under Cal. Civil Code § 1798.29 each of the aforementioned applies to DocuSign only as they pertain to DocuSign's performance as a processor service provider.

"**California Confidentiality Laws**" shall mean the applicable laws of the State of California governing the confidentiality, privacy, or security of PHI or other personally identifiable information (PII), including, but not limited to, the California Confidentiality of Medical Information Act (Cal. Civil Code § 56 et seq.), the patient access law (Cal. Health & Safety Code § 123100 et seq.), the HIV test result confidentiality law (Cal. Health & Safety Code § 120975 et seq.), the Lanterman-Petris-Short Act (Cal. Welf. & Inst. Code § 5328 et seq.), and California's data breach law (Cal. Civil Code § 1798.29) which apply to DocuSign only as they pertain to DocuSign's performance as a processor service provider.

"**HIPAA**" means, collectively, the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations (referred to herein as the "**HIPAA Rules**"), including the Privacy Rule, the Breach Notification Rule, the Security Rule and the Enforcement Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health (HITECH) Act and by the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act: Other modifications to the HIPAA Rules; Final Rule (commonly referred to as the Omnibus Final Rule).

"Privacy Breach" means any acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted or allowed under HIPAA or California Confidentiality Laws.

"**Privacy Rule**" means 45 CFR Part 160 and Subparts A and E of 45 CFR Part 164.

"**Protected Health Information**" ("**PHI**") or "**Electronic Protected Health Information**" ("**ePHI**") has the same meaning as the term "protected health information" or "electronic protected health information," respectively, in 45 CFR § 160.103; provided that, for purposes of this BAA, such term is limited to protected health information that is received and maintained by DocuSign from or on behalf of Customer via Customer's DocuSign Account.

"**Security Rule**" means Subpart C of 45 CFR Part 164.

"**Unsuccessful Security Incidents**" means, without limitation, pings and other broadcast attacks on DocuSign'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 PHI.

2. Permitted Uses and Disclosures by DocuSign

2.1 Performance under the Agreement. Subject to the requirements set forth in this BAA, DocuSign may Use and Disclose PHI for, or on behalf of, Customer as specified under the Agreement, provided such Use or Disclosure would not violate the Privacy and Security Rules or this BAA or California Confidentiality Laws. as specified under the Agreement.

2.2 Required by Law. DocuSign may Use or Disclose PHI as Required by Law or to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

2.3 Minimum Necessary. DocuSign agrees to make Uses and Disclosures and requests for PHI consistent with the Minimum Necessary policies and procedures required by HIPAA.

2.4 Management, Administration, and Legal Responsibilities. DocuSign may not Use or Disclose PHI in a manner that would violate the Privacy Rule if done by the Customer, except for the specific Uses and Disclosures set forth below.

(a) DocuSign may Use PHI for the proper management and administration of DocuSign or to carry out the legal responsibilities of DocuSign.

(b) DocuSign may Disclose PHI for the proper management and administration of DocuSign or to carry out the legal responsibilities of DocuSign, provided the Disclosures are Required by Law, or DocuSign obtains reasonable assurances from the person to whom the information is Disclosed that the information will remain confidential and will be Used or further Disclosed only as Required by Law or for the purposes for which it was Disclosed to the person, and the person notifies DocuSign of any instances of which it is aware in which the confidentiality of the information has been breached.

2.5 De-Identified Data. Intentionally omitted.

2.6 Data Aggregation. DocuSign may provide data aggregation services relating to the health care operations of the Customer, unless prohibited by the Agreement and as permitted by 45 C.F.R. Section 164.504(e)(4)(i);

3. DocuSign's Obligations

3.1 Prohibited Use and Disclosure. DocuSign will not Use or Disclose PHI other than as permitted or required by the Agreement and this BAA, or as otherwise Required by Law.

3.2 Safeguards. DocuSign will use reasonable and appropriate safeguards, including encryption in transit and at rest, and comply with the requirements of the Security Rule with respect to ePHI, to prevent the Use or Disclosure of PHI other than as provided for by the Agreement and this BAA.

3.3 Reporting and Notification

(a) Reporting. In the event of a Privacy Breach of Unsecured Protected Health Information or Security Incident, DocuSign will, within (5) business days of DocuSign's discovery, report the following in writing (including by email) to Privacy Officer of Customer:

(i) Any Privacy Breach of Unsecured Protected Health Information in accordance with and to the extent required by Federal law, including, but not limited to 45 C.F.R. § 164.410

(Notification by a business associate);

(j) Any breach of the security of the system of DocuSign involving the personal information provided by Customer, as such terms are defined in Cal. Civ. Code **§ 1798.29, in order for Customer to satisfy its California reporting obligations.**

(iii) Any Security Incidents involving ePHI of which DocuSign becomes aware and in which there is a successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference of the system operations associated with Customer's DocuSign Account in a manner that risks the confidentiality, integrity, or availability of such ePHI; provided, however, that DocuSign will not be obligated to report Unsuccessful Security Incidents and/or Security Incidents caused by Customer or Customer's Authorized Users..

(iv) Any Use or Disclosure of Customer's PHI that is not permitted or required by the Agreement and this BAA of which DocuSign becomes aware.

(b) Notification. Customer will be solely responsible for determining whether to notify impacted Individuals as well as determining whether the media and/or the Secretary must be notified, and for providing any such notices. As information is collected or otherwise becomes available to DocuSign and unless prohibited by law, DocuSign shall provide information regarding the nature and consequences of the Privacy Breach of Unsecured Protected Health Information that are reasonably requested to allow Customer to notify affected Individuals and/or government agencies. Due to the encryption configuration and security controls associated with the DocuSign Services, DocuSign may not have access to or know the nature of PHI contained within Customer's encrypted eDocuments. As such, the Parties acknowledge that it may not be possible for DocuSign to provide Customer with all relevant information concerning the PHI of Individuals who may have been affected by a Security Incident or Privacy Breach of Unsecured Protected Health Information.

3.4 Access, Amendment, and Accounting. DocuSign Services provide functionality to assist Customer insofar as this is possible, to access, amend, or provide an accounting of disclosures of PHI contained in DocuSign Services to respond to requests by an Individual. Should DocuSign receive any such requests directly from an Individual, DocuSign will advise such Individual to submit the Individual's request to Customer and Customer will be responsible for responding to any such request in accordance with 45 CFR § 164.524, 45 CFR § 164.526, and 45 CFR § 164.528 (as applicable) in a manner consistent with the functionality of the applicable DocuSign Services and the terms of the Agreement. To the extent Customer, in its use of the DocuSign Services, is not familiar with functionality that may be used for these purposes, DocuSign will provide Customer with reasonable additional Documentation or customer support to assist the Customer on how to take such actions in a manner consistent with the functionality of DocuSign Services and in accordance with the terms of the Agreement.

3.5 Subcontractors. DocuSign will ensure that any Subcontractors that create, receive, maintain, or transmit Customer's PHI on behalf of DocuSign agree to restrictions, requirements, and conditions that are at least as stringent or the same as those found in this BAA.

3.6 Audit Rights. DocuSign will make its internal practices, records, and books relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining compliance with the HIPAA Rules. Nothing in this section will be deemed to waive any applicable privilege or protection with respect to trade secrets and Confidential Information.

4. Customer's Responsibilities

In addition to any other obligations set forth in this BAA and the Agreement, Customer shall:

(a) implement and maintain appropriate administrative, physical and technical safeguards as required by the Security Rule;

(b) obtain any consent or authorization that may be required by HIPAA prior to furnishing PHI to DocuSign and, without limiting Customer's obligations under 4(c) below, abide by, and notify DocuSign of, any changes in, or revocation of, the permission by an Individual to Use or Disclose his or her PHI, to the extent that such changes may affect DocuSign's Use or Disclosure of PHI;

(c) be responsible for complying with any additional requests, restrictions or limitations relating to PHI that are agreed to by Customer with an Individual, with which Customer is required to abide by under 45 CFR 164.522, and/or that are set forth in any Notice of Privacy Practices prepared by or agreed to by Customer;

(d) not request or cause DocuSign (either directly or via the DocuSign Account) to Use or Disclose PHI in any manner that would not be permissible under HIPAA if done by a Covered Entity or Business Associate; and

(e) provide to DocuSign only the minimum PHI necessary for the provision and use of the DocuSign Services and shall not provide PHI to DocuSign outside of its Account (Example: Customer and its Authorized Users will not place PHI in emails and messages to DocuSign's support teams outside of its Account).

5. Term and Termination

5.1 Term. This BAA will commence on the effective date of the Agreement and will continue until the earlier of: (a) termination of this BAA by either Party for breach as set forth in Section 5.2 below; (b) notification to DocuSign by Customer that the DocuSign Account is no longer subject to this BAA, which, for clarification, will not terminate any then-current Order Forms; or (c) expiration or termination of the Agreement.

5.2 Termination for Breach. A material breach of this BAA will be treated as a material breach of the Agreement and, in the event of such breach (subject to the cure provision in the Agreement), the termination provisions of the Agreement will apply.

5.3 Effect of Termination. DocuSign will store and delete Customer's encrypted eDocuments that may contain Customer PHI in accordance with the terms set forth in the Agreement. If and to the extent DocuSign maintains possession of Customer PHI following the expiration or termination of this BAA, DocuSign will, at Customer's request return or destroy such PHI. If it is not feasible to return or destroy PHI in DocuSign's possession, then DocuSign will continue to apply to the protections of this BAA which shall survive termination or expiration of the Agreement and limit any further Use or Disclosure of the PHI to those purposes that make the return or destruction of the PHI infeasible.

6. 42 CFR Part 2 Substance Use Records

If and to the extent that Customer's eDocuments contain PHI that identifies an Individual as having an alcohol or drug use diagnosis or as having received treatment related thereto that is protected under 42 USC §290dd-2 and 42 C.F.R. Part 2 ("**Part 2**"), the following shall apply:

(a) DocuSign acknowledges and agrees that (i) if deemed a Qualified Service Organization under Part 2, it is fully bound by the Part 2 regulations with respect to such PHI and will Use and Disclose such PHI only as permitted by this BAA; and (ii) should DocuSign receive any requests for access to Customer's PHI by a third party, it will advise such third party to submit its request to Customer and will, if necessary and as permitted by applicable law, cooperate with Customer to resist in any efforts made in judicial proceedings to obtain access to Customer's PHI.

(b) Customer acknowledges and agrees that it is solely responsible for (i) obtaining all necessary authorizations, consents, and other permissions that may be required under Part 2 in order to maintain, transmit, or otherwise process PHI via its DocuSign Account; and (ii) determining whether any notices or disclosures with respect to its PHI are required under Part 2 and for providing any such notices or disclosures.

7. General

7.1 Mitigation. In the event of a Breach resulting in the unauthorized Use or Disclosure of Unsecured Protected Health Information in violation of this BAA, both Parties will, to the extent practicable under the circumstances, make commercially reasonable efforts to mitigate the harmful effects resulting from such breach.

7.2 Survival: The obligations of DocuSign under the provisions of Sections 3.1-3.6, and 5.3 and Section 7 shall survive termination of this BAA until such time as all PHI is returned to Customer or destroyed.

7.3 Amendments: This BAA may not be modified or amended, except in a writing duly signed by authorized representatives of the Parties. To the extent that any relevant provision of HIPAA is materially amended in a manner that changes the obligations of the Parties, the Parties agree to negotiate in good faith appropriate amendment(s) to this BAA to give effect to the revised obligations. Further, no provision of this BAA shall be waived, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

7.4 No Third Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor will anything in this BAA confer, upon any person other than the Parties, and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

7.5 Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below, and/or via facsimile or email to the facsimile telephone numbers or email addresses listed below.

If to DocuSign, to:

Attn: Data Privacy Officer
221 Main Street, #1550
San Francisco CA 94105
Phone:
Fax:
Email: privacy@docusign.com

If to Covered Entity, to:

County of Monterey Health Department Attn:
Compliance/Privacy Officer
1270 Natividad Road
Salinas, CA 93906
Phone: 831-755-4018
Fax: 831-755-4797
Email: sumeshwarsd@co.monterey.ca.us

Each Party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner hereinabove provided. Such notice is effective upon receipt of notice, but receipt is deemed to occur on next business day if notice is sent by FedEx or other overnight delivery service.

7.6 **Relationship of Parties.** Notwithstanding anything to the contrary in the Services Agreement, DocuSign is an independent contractor and not an agent of Customer under this BAA. DocuSign has the sole right and obligation to supervise, manage, contract, direct, procure, perform, or cause to be performed all Business Associate obligations as set forth under this BAA.

7.7 **Choice of Law; Interpretation**. This BAA shall be governed by the laws of the State of California. Any ambiguities in this BAA shall be resolved in a manner that allows Customer and DocuSign to comply with HIPAA and the California Confidentiality Laws as they apply to each party's respective role (which in the case of DocuSign is as a processor service provider).

7.8 **Indemnification**. DocuSign shall indemnify, defend, and hold harmless the County of Monterey (the "County"), in accordance with Section 9.3 of the Agreement (Procedures) its officers, agents, and employees from any claim, liability, loss, injury, cost, expense, penalty or damage, including costs incurred by the County with respect to any investigation, enforcement proceeding, or third party action, arising out of, or in connection with, a breach of the privacy safeguards of this BAA, resulting in the unauthorized use, access or disclosure of Customer's PHI that is attributable to an act or omission of DocuSign and/or its agents, members, employees, or Subcontractors, excepting only loss, injury, cost, expense, penalty or damage caused by the negligence or willful misconduct of personnel employed by the County. This provision is in addition to, and independent of, any indemnification provision in any Agreement between the Parties.

7.9 **Insurance.** In addition to any general and/or professional liability insurance required of DocuSign under the Agreement, DocuSign agrees to obtain and maintain, at its sole expense, liability insurance on an occurrence basis, covering any and all claims, liabilities, demands, damages, losses, costs expenses, fines, and compliance costs arising from a breach of the obligations of DocuSign, its officers, employees, agents and Subcontractors under this BAA as set forth in this Section 7.9 (Insurance). DocuSign's required insurance under this Section 7.10 shall include combined Errors & Omissions and Cyber Liability insurance covering breach notification expenses, network security and privacy liability, with limits of not less than $5,000,000 per claim and in the aggregate for E&O/Cyber on a combined basis. Such insurance coverage will be maintained for the term of this BAA, and a copy of such policy or a certificate evidencing the policy shall be provided to Covered Entity at Covered Entity's request.

7.10 **Audit or Investigations.** Promptly, but no later than five (5) calendar days after notice thereof, DocuSign shall advise Customer of any audit, compliance review, or complaint investigation by the Secretary or other state or federal agency related to compliance with HIPAA

7.11 Reserved
7.12 Reserved.

7.13 **No Offshore Work**. In performing the Services for, or on behalf of, Customer, DocuSign shall not, and shall not permit any of its Subcontractors, to transmit or make available any PHI to any entity or individual outside the United States without the prior written consent of Covered Entity. Customer acknowledges that that when it sends envelopes to persons outside of the United States then it will have consented to cross border transfer of any Personal Information contained therein.

7.14 **Interpretation.** It is the Parties' intent that any ambiguity under this BAA be interpreted in accordance with HIPAA and applicable California Confidentiality Laws, and the HIPAA Rules, as each is amended from time to time.

7.15 Entire Agreement. This BAA is the final, complete, and exclusive expression of the agreement between the Parties regarding the subject matter hereof, and supersedes and replaces any prior business associate agreement that may have been in effect between the Parties. This BAA may be changed only by a written agreement signed by an authorized agent of both Parties.

The Parties' respective authorized signatories hereby agree to the terms and conditions of this BAA effective as of the BAA Effective Date.

Customer: County of Monterey, a political subdivision of the State of California, on behalf of Monterey County Health Department	**DocuSign, Inc.**
By: _____	By: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____