

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) effective _____, 20__ (“Effective Date”), is entered into by and among between the County of Monterey, a political subdivision of the State of California, on behalf of the Health Department (“Covered Entity”) and _____ (“Business Associate”) (each a “Party” and collectively the “Parties”).

RECITALS

A. WHEREAS, Business Associate provides certain services for Covered Entity that involve the Use and Disclosure of Protected Health Information (“PHI”) that is created, received, transmitted, or maintained by Business Associate for or on behalf of Covered Entity.

B. WHEREAS, the Parties are committed to complying with the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), and their implementing regulations, including the Standards for the Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, subparts A and E (the “Privacy Rule”), the Breach Notification Standards, 45 C.F.R. Part 160 and 164 subparts A and D (the “Breach Notification Rule”), and the Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, subparts A and C (the “Security Rule”) (collectively “HIPAA”), all as amended from time to time.

C. WHEREAS, the Parties are also committed to complying with the California Confidentiality Laws (defined below).

D. WHEREAS, to the extent that Business Associate is performing activities in connection with covered accounts for or on behalf of Covered Entity, the Parties are also committed to complying with applicable requirements of the Red Flag Rules issued pursuant to the Fair and Accurate Credit Transactions Act of 2003 (“Red Flag Rules”).

E. WHEREAS, the Privacy and Security Rules require Covered Entity and Business Associate to enter into a business associate agreement that meets certain requirements with respect to the Use and Disclosure of PHI. This BAA sets forth the terms and conditions pursuant to which PHI, and, when applicable, Electronic Protected Health Information (“EPHI”) shall be handled, in accordance with such requirements.

NOW THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this BAA, the Parties agree as follows:

AGREEMENT

1. **DEFINITIONS**

All capitalized terms used in this BAA but not otherwise defined shall have the meaning set forth in HIPAA.

(a) “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.

(b) “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).

(c) “Protected Health Information” or “PHI” shall mean any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual; (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information that can be used to identify the individual, and (iii) is provided by Covered Entity to Business Associate or created, maintained, received, or transmitted by Business Associate on Covered Entity’s behalf. PHI, when used in this BAA, includes EPHI.

(d) “Services” shall mean the services for or functions performed by Business Associate on behalf of Covered Entity pursuant to an underlying services agreement (“Services Agreement”) between Covered Entity and Business Associate to which this BAA applies.

2. PERMITTED USES AND DISCLOSURES OF PHI

Unless otherwise limited herein, Business Associate may:

(a) Use or Disclose PHI to perform Services for, or on behalf of, Covered Entity, provided that such Use or Disclosure would not violate the Privacy or Security Rules, this BAA, or California Confidentiality Laws if done by Covered Entity;

(b) Use PHI to provide Data Aggregation Services for the Health Care Operations of Covered Entity, if required by the Services Agreement and as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B);

(c) Use PHI if necessary for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate as permitted by 45 C.F.R. § 164.504(e)(4)(i);

(d) Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate as

permitted under 45 C.F.R. § 164.504(e)(4)(ii), provided that Disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will remain confidential and be Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and that such person will notify the Business Associate of any instances of which such person is aware that the confidentiality of the information has been breached; and

(e) Use PHI to report violations of law to appropriate Federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

3. RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PHI

3.1. Responsibilities of Business Associate. Business Associate shall:

(a) Notify the Privacy Officer of Covered Entity, in writing, of: (i) any Use and/or Disclosure of the PHI that is not permitted by this BAA; (ii) any Security Incident of which Business Associate becomes aware; and (iii) any suspected Breach. Such notice shall be provided within five (5) business days of Business Associate's discovery of such unauthorized access, acquisition, Use and/or Disclosure, Security Incident, or suspected Breach. Notwithstanding the foregoing, the Parties acknowledge the ongoing existence and occurrence of attempted but ineffective Security Incidents that are trivial in nature, such as pings and other broadcast service attacks, and unsuccessful log-in attempts. The Parties acknowledge and agree that this Section 3.1(a) constitutes notice by Business Associate to Covered Entity of such ineffective Security Incidents and no additional notification to Covered Entity of such ineffective Security Incidents is required, provided that no such Security Incident results in unauthorized access, acquisition, Use or Disclosure of PHI. For the avoidance of doubt, a ransomware attack shall not be considered an ineffective Security Incident and shall be reported to Covered Entity, irrespective of whether such Security Incident results in a Breach. Business Associate shall investigate each Security Incident or unauthorized access, acquisition, Use, or Disclosure of PHI, or suspected Breach that it discovers and shall provide a summary of its investigation to Covered Entity, upon request;

(i) If Business Associate or Covered Entity determines that such Security Incident or unauthorized access, acquisition, Use, or Disclosure, or suspected Breach constitutes a Breach, then Business Associate shall provide a supplemental written report in accordance with 45 C.F.R. § 164.410(c), which shall include, to the extent possible, the identification of each individual whose PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, Used or Disclosed during the Breach, to Covered Entity without unreasonable delay, but no later than five (5) business days after discovery of the Breach;

(ii) In consultation with Covered Entity, Business Associate shall promptly mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of such improper access, acquisition, Use, or Disclosure, Security Incident, or Breach; and

(iii) Covered Entity shall have sole control over the timing and method of providing notification of such Breach to the affected individual(s), the appropriate government agencies, and other persons required by law to be notified. Business Associate shall assist with any notifications, as requested by Covered Entity. Business Associate shall take prompt corrective action, including any action required by applicable State or federal laws and regulations relating to such Security Incident or non-permitted access, acquisition, Use, or Disclosure. Business Associate shall reimburse Covered Entity for its reasonable costs and expenses in providing notification to affected individuals, appropriate government agencies, and any other persons required by law to be notified (e.g., without limitation, the media or consumer reporting agencies), including, but not limited to, any administrative costs associated with providing notice, printing and mailing costs, public relations costs, attorney fees, and costs of mitigating the harm (which may include the costs of obtaining up to one (1) year of credit monitoring services and identity theft insurance) for affected individuals whose PHI or other PII has or may have been compromised as a result of the Breach.

(b) Implement appropriate administrative, physical, and technical safeguards and comply with the Security Rule and industry best practices to prevent Use and/or Disclosure of EPHI other than as provided for by this BAA;

(c) Obtain and maintain a written agreement with each of its Subcontractors that creates, receives, maintains, or transmits PHI that requires each such Subcontractor to adhere to restrictions and conditions that are at least as restrictive as those that apply to Business Associate pursuant to this BAA. Upon request, Business Associate shall provide Covered Entity with copies of its written agreements with such Subcontractors;

(d) Make available all internal practices, records, books, agreements, policies and procedures and PHI relating to the Use and/or Disclosure of PHI received from, created, maintained, or transmitted by Business Associate on behalf of Covered Entity to the Secretary of the Department of Health and Human Services (“Secretary”) in a time and manner designated by the Secretary for purposes of determining Covered Entity’s or Business Associate’s compliance with HIPAA. Business Associate shall immediately notify Covered Entity of any such requests by the Secretary and, upon Covered Entity’s request, provide Covered Entity with any copies of documents Business Associate provided to the Secretary. In addition, Business Associate shall promptly make available to Covered Entity such practices, records, books, agreements, policies and procedures relating to the Use and Disclosure of PHI for purposes of determining whether Business Associate has complied with this BAA or maintains adequate security safeguards, upon reasonable request by Covered Entity. The fact that Covered Entity has the right to inspect, inspect, or fails to inspect Business Associate’s internal practices, records, books, agreements, policies and procedures does not relieve Business Associate of its responsibility to comply with this BAA, regardless of whether Covered Entity detects or fails to detect a violation by Business Associate, nor does it constitute Covered Entity’s acceptance of such practices or waiver of Covered Entity’s rights under this BAA;

(e) Document Disclosures of PHI and information related to such Disclosure and, within twenty (20) days of receiving a written request from Covered Entity, provide to Covered Entity such information as is requested by Covered Entity to permit Covered Entity to respond to a request by an individual for an accounting of the Disclosures of the individual's PHI in accordance with 45 C.F.R. § 164.528 and the HITECH Act. At a minimum, the Business Associate shall provide Covered Entity with the following information: (i) the date of the Disclosure; (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (iii) a brief description of the PHI Disclosed; and (iv) a brief statement of the purpose of such Disclosure which includes an explanation of the basis for such Disclosure. In the event the request for an accounting is delivered directly to the Business Associate, the Business Associate shall, within ten (10) days, forward such request to Covered Entity. The Business Associate shall implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section;

(f) Subject to Section 4.4 below, return to Covered Entity in a mutually agreeable format and medium, or destroy, within thirty (30) days of the termination of this BAA, the PHI in its possession and retain no copies, including backup copies;

(g) Use, Disclose to its Subcontractors or other third parties, and request from Covered Entity, only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder;

(h) If all or any portion of the PHI is maintained in a Designated Record Set;

(i) Upon ten (10) days' prior written request from Covered Entity, provide access to the PHI to Covered Entity, or to the individual, if so directed by Covered Entity, to meet a request by an individual under 45 C.F.R. § 164.524 or California Confidentiality Laws. Business Associate shall notify Covered Entity within five (5) days of its receipt of a request for access to PHI from an individual; and

(ii) Upon ten (10) days' prior written request from Covered Entity, make any amendment(s) to the PHI that Covered Entity directs pursuant to 45 C.F.R. § 164.526. Business Associate shall notify Covered Entity within five (5) days of its receipt of a request for amendment of PHI from an individual.

(i) If applicable, maintain policies and procedures to detect and prevent identity theft in connection with the provision of the Services, to the extent required to comply with the Red Flag Rules;

(j) To the extent that Business Associate carries out one or more of Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations;

(k) Unless prohibited by law, notify Covered Entity as soon as possible and in no case later than five (5) days after the Business Associate's receipt of any request

or subpoena for PHI. To the extent that Covered Entity decides to assume responsibility for challenging the validity of such request, the Business Associate shall cooperate fully with Covered Entity in such challenge; and

(l) Maintain policies and procedures materially in accordance with HIPAA and California Confidentiality Laws and industry standards designed to ensure the confidentiality, availability, and integrity of Covered Entity's data and protect against threats or vulnerabilities to such data.

3.2 Business Associate Acknowledgment.

(a) Business Associate acknowledges that, as between the Business Associate and Covered Entity, all PHI shall be and remain the sole property of Covered Entity.

(b) Business Associate is not permitted to Use PHI to create de-identified information except as approved in writing by Covered Entity.

(c) Business Associate further acknowledges that it is obligated by law to comply, and represents and warrants that it shall comply, with HIPAA. Business Associate shall comply with all California Confidentiality Laws, to the extent that such state laws are not preempted by HIPAA.

(d) Business Associate further acknowledges that Uses and Disclosures of PHI must be consistent with Covered Entity's privacy practices, as stated in Covered Entity's Notice of Privacy Practices. The current Notice of Privacy Practices can be retrieved online from the Covered Entity's webpage. Business Associate agrees to review the Notice of Privacy Practices at this URL at least once annually while doing business with Covered Entity to ensure it remains updated on any changes to the Notice of Privacy Practices Covered Entity may make.

3.3 Responsibilities of Covered Entity. Covered Entity shall notify Business Associate of any (i) changes in, or withdrawal of, the authorization of an individual regarding the Use or Disclosure of PHI provided to Covered Entity pursuant to 45 C.F.R. § 164.508, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI; or (ii) restrictions on Use and/or Disclosure of PHI as provided for in 45 C.F.R. § 164.522 agreed to by Covered Entity, to the extent that such restriction may affect Business Associate's Use or Disclosure of PHI.

4. TERM AND TERMINATION

4.1 Term. This BAA shall become effective on the Effective Date and shall continue in effect until all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or if it is infeasible to return or destroy PHI, protections are extended to such PHI, in accordance with the termination provisions in Section 4.4. Certain provisions and requirements of this BAA shall survive its expiration or other termination as set forth in Section 5 herein.

4.2 Termination. If Covered Entity determines in good faith that Business Associate has breached a material term of this BAA, Covered Entity may either: (i) immediately terminate this BAA and any underlying Services Agreement without penalty; or (ii) terminate this BAA and any underlying Services Agreement within thirty (30) days of Business Associate's receipt of written notice of such breach, if the breach is not cured to the satisfaction of Covered Entity.

4.3 Automatic Termination. This BAA shall automatically terminate without any further action of the Parties upon the termination or expiration of all Services Agreements between Covered Entity and Business Associate that would necessitate having this BAA in place.

4.4 Effect of Termination. Upon termination or expiration of this BAA for any reason, Business Associate shall return or destroy all PHI pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(J) if, and to the extent that, it is feasible to do so. Prior to returning or destroying the PHI, Business Associate shall recover any PHI in the possession of its Subcontractors. Business Associate shall certify in writing that all PHI has been returned or securely destroyed, and no copies retained, upon Covered Entity's request. To the extent it is not feasible for Business Associate to return or destroy any portion of the PHI, Business Associate shall notify Covered Entity in writing of the condition that makes return or destruction infeasible. If Covered Entity agrees that return or destruction of the PHI is infeasible, as determined in its sole discretion, Business Associate shall: (i) retain only that PHI which is infeasible to return or destroy; (ii) return to Covered Entity the remaining PHI that the Business Associate maintains in any form; (iii) continue to extend the protections of this BAA to the PHI for as long as Business Associate retains PHI; (iv) limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction of the PHI not feasible and subject to the same conditions as set out in Sections 2 and 3 above, which applied prior to termination; and (v) return to Covered Entity the PHI retained by Business Associate when such return is no longer infeasible.

5. MISCELLANEOUS

5.1 Survival. The obligations of Business Associate under the provisions of Sections 3.1, 3.2, and 4.4 and Article 5 shall survive termination of this BAA until such time as all PHI is returned to Covered Entity or destroyed.

5.2 Amendments: Waiver. 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 or California Confidentiality Laws 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.

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

5.4 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 Business Associate, to:

 Attn: _____

 Phone: _____
 Fax: _____
 Email: _____

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.

5.5 Counterparts: Facsimiles. This BAA may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile and electronic copies hereof shall be deemed to be originals.

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

5.7 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 Covered Entity and Business Associate to comply with HIPAA and the California Confidentiality Laws.

5.8 Indemnification. Business Associate shall indemnify, defend, and hold harmless the County of Monterey (the “County”), 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 violation of this BAA, HIPAA or California Confidentiality Laws, or a Breach that is attributable to an act or omission of Business Associate 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. It is the intent of the Parties to provide the broadest possible indemnification for the County. This provision is in addition to, and independent of, any indemnification provision in any Services Agreement between the Parties.

5.9 Applicability of Terms. This BAA applies to all present and future Services Agreements and business associate relationships, written or unwritten, formal or informal, in which Business Associate creates, receives, transmits, or maintains any PHI for or on behalf of Covered Entity in any form whatsoever. This BAA shall automatically be incorporated in all subsequent agreements between Business Associate and Covered Entity involving the Use or Disclosure of PHI whether or not specifically referenced therein. In the event of any conflict or inconsistency between a provision of this BAA and a provision of any other agreement between Business Associate and Covered Entity, the provision of this BAA shall control unless the provision in such other agreement establishes additional rights for Business Associate or additional duties for or restrictions on Business Associate with respect to PHI, in which case the provision of such other agreement will control.

5.10 Insurance. In addition to any general and/or professional liability insurance required of Business Associate under the Services Agreement, Business Associate 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 Business Associate, its officers, employees, agents and Subcontractors under this BAA. Without limiting the foregoing, at a minimum, Business Associate’s required insurance under this Section shall include cyber liability insurance covering breach notification expenses, network security and privacy liability. The insurance coverage limits, per claim and in the aggregate, shall not be less than the following amounts based upon the number of unique patient served under this agreement:

Unique Patients	Coverage
Less than 12,001	\$2,000,000
12,001 – 30,000	\$3,000,000
30,001 – 60,000	\$5,000,000
More than 60,000	\$10,000,000

If the Business Associate maintains broader coverage and/or higher limits than these minimums, the Covered Entity requires, and shall be entitled to, the broader coverage and/or the higher limits maintained by the Business Associate. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be

available to the Covered Entity. 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.

5.11 Legal Actions. Promptly, but no later than five (5) calendar days after notice thereof, Business Associate shall advise Covered Entity of any actual or potential action, proceeding, regulatory or governmental orders or actions, or any material threat thereof that becomes known to it that may affect the interests of Covered Entity or jeopardize this BAA, and of any facts and circumstances that may be pertinent to the prosecution or defense of any such actual or potential legal action or proceeding, except to the extent prohibited by law. This includes, without limitation, any allegation that Business Associate has violated HIPAA or other federal or state privacy or security laws.

5.12 Audit or Investigations. Promptly, but no later than five (5) calendar days after notice thereof, Business Associate shall advise Covered Entity of any audit, compliance review, or complaint investigation by the Secretary or other state or federal agency related to compliance with HIPAA or the California Confidentiality Laws.

5.13 Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself, and any Subcontractors, employees, or agents assisting Business Associate in the performance of its obligations under any Services Agreements, available to Covered Entity, at no cost to Covered Entity, to testify in any claim commenced against Covered Entity, its directors, officers, employees, successors, and assigns based upon claimed violation by Business Associate or its agents or subcontractors of HIPAA or other applicable law, except where Business Associate or its Subcontractor, employee, or agent is a named adverse party.

5.14 No Offshore Work. In performing the Services for, or on behalf of, Covered Entity, Business Associate 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.

5.15 Information Blocking Rules. Business Associate shall not take any action, or refuse to take any action, with regard to Covered Entity's electronic health information that would result in "information blocking" as prohibited by 42 U.S.C. § 300jj-52 and 45 C.F.R. Part 171 (collectively, "Information Blocking Rules"). Business Associate and Covered Entity shall cooperate in good faith to ensure Covered Entity's electronic health information is accessed, exchanged, and used in compliance with the Information Blocking Rules.

IN WITNESS WHEREOF, each of the undersigned has caused this BAA to be duly executed in its name and on its behalf as of the Effective Date.

BUSINESS ASSOCIATE

COVERED ENTITY

By: _____ By: _____

Print Name _____ Print Name: _____

Print Title _____ Print Title: _____

Date: _____ Date: _____

.

DocuSigned by:
Shane Eben Strong
6624564F383643C...
Shane Eben Strong

office of County Counsel
2/9/2024 | 8:07 PM PST