# Business Associate Agreement

Sutter Health

## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (this "**Agreement**") is by and between **Sutter Health**, a California nonprofit public benefit corporation ("**Sutter Health**"), on behalf of itself, its Affiliates and the Sutter Health Affiliated Covered Entity (as defined below), as such may be amended from time to time (collectively, "**Sutter**"), and _____ ("**Business Associate**") (each a "**Party**" and collectively, the "**Parties**"), and is effective as of _____ (the "**Effective Date**").

## RECITALS

**A.** For purposes of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended, Sutter Health designated itself and certain of its Affiliates that are covered entities (as defined at 45 C.F.R. § 160.103) as an Affiliated Covered Entity, in accordance with 45 C.F.R. § 164.105(b) (the "Sutter Health Affiliated Covered Entity").

**B.** Sutter and Business Associate have entered into current arrangements or may enter into future arrangements (collectively, "Underlying Service Agreements") in which Business Associate provides services to, or performs functions on behalf of, Sutter which involve the Use or Disclosure of, or Business Associate creating, receiving, maintaining, or transmitting, Protected Health Information on behalf of Sutter, consistent with the definition of "business associate" at 45 C.F.R. § 160.103.

**C.** The Parties desire to comply with federal and state laws regarding the collection, Use, Disclosure, and safeguarding, including ensuring the confidentiality, integrity, and availability, of individually identifiable health information and personal information, in particular with the provisions of the federal Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and implementing regulations (collectively, "HIPAA").

## AGREEMENT

Now, therefore, in consideration of the promises set forth herein and in the Underlying Service Agreements, the delivery and sufficiency of which is acknowledged, the Parties agree as follows:

**1.** Definitions. The Parties agree that any capitalized terms shall have the same definition as given to them under HIPAA, unless specified otherwise herein.

a. Affiliate: For purposes of this Agreement, a legal entity is an "Affiliate" of Sutter Health if it directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with Sutter Health.

b. Protected Health Information: Protected Health Information shall have the same meaning as "protected health information" at 45 C.F.R. § 160.103 that is disclosed to Business Associate by Sutter or created, received, maintained, or transmitted by Business Associate, or any Subcontractor, on behalf of Sutter, and shall also include "medical information" as defined at Cal. Civil Code § 56.05. Collectively, this information is referred to herein as PHI.

**2.** Obligations of Business Associate. Business Associate agrees that it shall keep confidential and safeguard all information protected under federal or state laws, including but not limited to PHI. Business Associate shall perform all obligations under this Agreement in strict compliance with HIPAA, California law, and all other applicable laws. Business Associate shall be solely responsible for complying with HIPAA and all other applicable laws.

a. Safeguards: Business Associate shall comply with Subpart C of 45 C.F.R. Part 164 ("Security Rule") with respect to electronic PHI, including implementing applicable administrative, technical, and physical safeguards and other applicable requirements, to ensure the Confidentiality, Integrity, and Availability of all electronic PHI and to prevent any Use or Disclosure of electronic PHI other than as provided for by this Agreement.



Sutter Health

b. Policies and Procedures; Training: Business Associate shall maintain and strictly adhere to policies and procedures as required under HIPAA and as necessary to protect the Confidentiality, Integrity and Availability of PHI and to prevent unauthorized Use or Disclosure of PHI. Business Associate shall ensure all Workforce members receive initial and periodic training on its privacy and information security policies and procedures.

c. Reporting: Business Associate shall report to Sutter any Use or Disclosure of PHI not provided for by this Agreement of which it becomes aware, including but not limited to Breaches of Unsecured PHI as required at 45 C.F.R. § 164.410, and any Security Incident within forty-eight (48) hours of discovery. Provided, however, that this Agreement shall serve as Business Associate's notice to Sutter for unsuccessful attempts at unauthorized Access, Use, Disclosure, modification, or destruction of PHI or unsuccessful attempts at interference with system operations in an information system, such as "pings" on a firewall.

   i. Reports shall include, to the extent possible: a description of what happened, including the date of the Discovery and date of the Breach, Use or Disclosure not permitted by this Agreement, or Security Incident; the types of PHI that were involved; the number of Individuals potentially impacted; any steps Individuals should take to protect themselves from potential harm; and what Business Associate is doing to investigate, mitigate, and protect against further unauthorized Use or Disclosure of PHI. Business Associate shall immediately supplement this report to Sutter if any information originally reported changes or if Business Associate learns of any additional information outlined above, including but not limited to a full list of names and addresses, or other contact information, for affected Individuals, to the extent that Business Associate maintains such information.

   ii. Business Associate shall cooperate with Sutter's reasonable requests for updates and additional information during the course of Business Associate or Sutter's investigation into a potential Use or Disclosure of PHI not permitted by this Agreement.

   iii. Reports required under section shall be made by phone and in writing, by certified mail or email, to the Sutter Health Chief Privacy and Information Security Officer, with supplemental reports made by email or as the Sutter Health Chief Privacy and Information Security Officer may otherwise direct:

Sutter Health, Chief Privacy Officer
2200 River Plaza Dr., 3rd Floor
Sacramento, CA 95833
Ph: (855) 771-4220
SHPI@sutterhealth.org

   iv. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Security Incident, or Use or Disclosure of PHI in violation of this Agreement.

d. Subcontractors: Business Associate shall ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree in writing to the same restrictions, conditions, and requirements that apply to Business Associate through this Agreement.

e. Transmission/Access Outside of the U.S.: Business Associate shall not store, access, Use or Disclose PHI, nor allow a Subcontractor to store, access, Use or Disclose PHI, outside of the United States of America without the express written consent of Sutter.

f. Access to PHI: Upon request by Sutter, Business Associate shall promptly provide PHI to Sutter within five (5) calendar days to permit any Individual whose PHI is maintained by or on behalf of Business Associate to have access to and to copy his/her PHI in accordance with 45 C.F.R. § 164.524, and applicable state law, including but not limited to California law. Such PHI shall be produced in the format requested by Sutter. If an Individual contacts Business Associate directly for such access, Business Associate shall direct the Individual to contact Sutter.

g. Amendment of PHI: Upon the request of Sutter, Business Associate shall amend PHI and/or make PHI available to Sutter within five (5) business days for amendment, and incorporate any amendments as instructed by Sutter as necessary to allow Sutter to comply with 45 C.F.R. § 164.526 and applicable state law, including California law. If an Individual contacts Business Associate directly to amend PHI, Business Associate shall direct the Individual to contact Sutter.

h. Accounting of Disclosures of PHI: Business Associate, and any Subcontractor acting on its behalf, must account for all Disclosures of PHI for which a Covered Entity must account for to comply with 45 C.F.R. § 164.528, as may be amended. Upon the request of Sutter, Business Associate shall provide to Sutter within five (5) business days an accounting of all Disclosures of PHI consistent with 45 C.F.R. § 164.528(b) in order for Sutter to comply with its legal obligations. If an Individual contacts Business Associate directly for such an accounting, Business Associate shall direct the Individual to contact Sutter.

i. Minimum Necessary: Business Associate and its Subcontractors shall request from Sutter and Use and Disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, Use, or Disclosure in accordance with 45 C.F.R. §§ 164.502(b) and 164.514(d).

j. Prohibition on Sale of PHI: Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI. Business Associate shall not obtain an authorization for the sale of PHI except as expressly permitted in writing from the Sutter Health Chief Privacy and Information Security Officer, and in accordance with the authorization requirements at 45 C.F.R. § 164.508 and Cal. Civ. Code 56.11.

k. Audits, Investigations, Inspections: As it relates to the Use and Disclosure of PHI received from, or created or received by, Business Associate on behalf of Sutter, Business Associate shall make its written agreements, internal practices, books, documents, and records to the Secretary of HHS ("Secretary"), and/or Sutter upon reasonable request.

l. Performance of Covered Entity Obligations: To the extent that Business Associate performs any of Sutter's obligations under HIPAA, Business Associate shall comply with the requirements that apply to a Covered Entity in the performance of such obligations.

m. Indemnification: Notwithstanding any limitation on damages or liability or any indemnification obligations contained in the Underlying Service Agreements between the Parties, each Party agrees to indemnify and defend, and hold harmless the other Party, its affiliates, and any of its or their officers, directors, attorneys, agents or employees, from all claims, costs, settlement fees, attorneys' fees, losses, damages, liabilities and penalties arising from or connected with the breach by the indemnifying Party or any of its officers, directors, agents, Subcontractors or employees, of its obligations under this Agreement.

n. Insurance: Business Associate agrees to purchase and maintain throughout the Term of this Agreement, Technology Errors & Omissions Insurance with minimum limits of $2,000,000 per claim, $2,000,000 aggregate. Business Associate also agrees to purchase and maintain throughout the term of this Agreement, Privacy & Security liability insurance (or its equivalent "cyber/network security" insurance) covering liabilities resulting or arising from acts, errors, or omissions, in connection with the services provided or permitted under this Agreement which are associated with any unlawful or unauthorized access to, or acquisition, Use or Disclosure of PHI, including any Use or Disclosure not permitted by this Agreement, and any Breach, loss or compromise of any PHI. Such insurance shall provide coverage with minimum limits of $5,000,000.00 per claim. Costs and damages to be covered by this insurance policy shall include without limitation: (a) costs to notify individuals, including but not limited to establishing a call center or similar process; (b) costs to provide credit monitoring and credit restoration services to individuals; (c) costs and damages associated with third party claims including restoration expenses, revenue loss, civil penalties, litigation costs and settlement costs; and (d) any investigation and enforcement costs, including but not limited to any forensic investigation costs. The policy must be kept in force during the life of this Agreement and for 6 years (either as a policy in force or extended reporting period) after Agreement termination.

o. Legal Process: Unless expressly prohibited by law, Business Associate shall cooperate with Sutter related to government or regulatory investigations, including reasonably anticipated investigations or inquiries. Business Associate shall immediately notify Sutter if Business Associate receives a request or notification from the Secretary or other government agency related to Sutter. In the event that Business Associate is served with legal process (e.g., a subpoena) or request from a government agency (e.g., the Secretary) that potentially could require the Disclosure of PHI, Business Associate shall provide prompt notice of such legal process to Sutter and cooperate with any of Sutter's challenges to such requests or legal process. In addition, Business Associate shall not Disclose the PHI without the express written consent of Sutter unless expressly permitted under this Agreement. Nothing in this Agreement shall be construed as a waiver of any legal privilege or any protections of trade secrets or confidential commercial information.

3. Uses and Disclosures of PHI by Business Associate.

   a. Business Associate shall not, and shall not permit any Subcontractor to, Use or Disclose PHI other than as permitted or required under this Agreement. Without limiting the foregoing, Business Associate shall only Use or Disclose PHI, and permit a Subcontractor to Use or Disclose PHI, as necessary to fulfill the specific terms of, or perform specific functions, activities, or services specified in, the Underlying Service Agreements, or for Business Associate's own proper management and administration, and to fulfill any of Business Associate's legal responsibilities

   b. Business Associate shall not Use or Disclose PHI in any manner that would violate HIPAA if done by a Covered Entity.

   c. Business Associate may not Use or Disclose PHI to create de-identified information, aggregate data, or anonymous or pseudonymous data for Business Associate's own use or purposes or for use with any third party.

4. Obligations of Sutter.

   a. Restrictions: Sutter shall notify Business Associate in writing of any restrictions on the Use or Disclosure of an Individual's PHI that Sutter has agreed to, including restrictions for which Sutter must agree to, that may affect Business Associate's performance of its obligations under this Agreement.

   b. Revocations: Sutter shall notify Business Associate in writing of any changes in, or revocation of, permission by an Individual relating to the Use or Disclosure of PHI, if such changes or revocation may affect Business Associate's performance of obligations under this Agreement. Such notification shall be made to:

      Name .....

      Address .....

5. Termination.

   a. Breach: If Business Associate breaches its obligations under this Agreement, without advance written notice, Sutter may terminate for cause this Agreement and the Underlying Service Agreements to the extent that the Underlying Service Agreements create a Business Associate relationship.

   b. Automatic Termination: This Agreement shall automatically terminate upon the mutual agreement of the Parties.

   c. Survival: Termination of this Agreement for any reason shall not relieve either party of any obligation or liability incurred prior to the termination of this Agreement. The following provisions shall survive termination of this Agreement, in addition to those that by their nature are intended to survive termination. i.e., INDEMNIFICATION, INSURANCE, LEGAL PROCESS, PROCEDURE UPON TERMINATION, and OWNERSHIP OF DATA.

   d. Procedure upon Termination: Within fourteen (14) days of the effective date of termination of this Agreement, Business Associate shall return all PHI that it, or a Subcontractor on its behalf, has created or received, or maintains in any form at no cost to Sutter, and shall retain no copies of PHI, except as provided below. Business Associate shall securely destroy any remaining copies of PHI that it or a Subcontractor on its behalf maintains, in accordance with HHS guidance and NIST Special Publication 800-88 for electronic media. Upon request, Business Associate shall certify to Sutter that Business Associate has destroyed and/or returned all PHI, in accordance with Sutter's request or as set forth above. If return or destruction of PHI is not feasible, Business Associate shall continue to extend the protections of this Agreement to the PHI, and limit further Use of the PHI to those purposes that make the return or destruction of the PHI infeasible.

6. Ownership of PHI. All PHI shall be and remain the property of Sutter.

7. Amendment; Consents; Approvals. The Parties agree to take such action as is necessary to amend this Agreement for Sutter to comply with HIPAA or other applicable law. The Parties agree that this Agreement may only be modified by mutual written amendment, signed by both Parties, effective on the date set forth in the amendment. Unless otherwise specified herein any written consent or approval from Sutter or Sutter Health required under this Agreement shall be provided by the Chief Privacy and Information Security Officer or her/his designee.

8. Independent Contractor. The Parties agree that Business Associate is an independent contractor, and not an employee, agent, or partner of, or joint venturer with, Sutter.

9. Entire Agreement. This Agreement (together with any recitals and exhibits, which are hereby incorporated by this reference) constitutes the entire understanding and agreement between the Parties relating to PHI, and it supersedes any and all prior or contemporaneous agreements, representations and understandings of the Parties, except that any other terms related to security controls or safeguards that are more stringent than those required by this Agreement or not addressed herein, including any attached/incorporated exhibit, shall control.

10. Waiver. Any failure of a Party to insist upon strict compliance with any provision of this Agreement shall not be deemed to be a waiver of such provision. To be effective, a waiver must be in writing, signed and dated by the Parties to this Agreement. No waiver by either Party shall be construed to be a continuing waiver of any provision of this Agreement.

11. Counterparts. This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and all of which together shall be deemed one and the same instrument. Any photocopy of this executed Agreement may be used as if it were the original.

12. Governing Law. Notwithstanding any other provision to the contrary, this Agreement shall be governed and construed in accordance with the laws of the State of California.

13. Interpretation. Any ambiguities shall be resolved to permit the Parties to comply with HIPAA and other applicable federal and state law.

14. Effect on Underlying Service Agreements. To the extent the Underlying Service Agreements conflict with or are inconsistent with this Agreement, this Agreement shall control.

15. Execution. By their respective signatures and execution dates, below, each of the following represents that he or she is duly authorized to execute this Agreement and to bind the Party on whose behalf such execution is made.

| **SUTTER HEALTH** | **BUSINESS ASSOCIATE** |
|---|---|
| Signature: ..... | Signature: ..... |
| Name: **Jacki Monson** | Name: ..... |
| Title: **Chief Privacy Officer** | Title: ..... |
| Date: ..... | Date: ..... |