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"), its Affiliates on behalf of those entities and the Sutter Health Affiliated Covered Entity, 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. Sutter and Business Associate have entered into 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.

B. The Parties desire to comply with federal and state laws, including but not limited to California 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. Individual: Individual shall have the same meaning as "individual" at 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

c. Protected Health Information: Protected Health Information shall have the same meaning as "protected health information" at 45 C.F.R. § 160.103 that is 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 and "personal information" as defined at Cal. Civil Code § 1798.80, and all metadata related to protected health information, medical information, and personal information. For the avoidance of doubt, personal information includes Sutter employee, other workforce member, or customer personal information as well as patient and member personal information. Collectively, this information is referred to 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 that Business Associate receives from, or creates or receives on behalf of, Sutter. Business Associate warrants that it will 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. Sutter is not responsible for determining or monitoring Business Associate's compliance.

Sutter Health

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, physical, and technical 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. Business Associate also shall comply with the requirements set forth at 45 C.F.R. 164.530(c) for safeguarding PHI. Additionally, Business Associate shall comply with the specific information security requirements set forth in the attached Information Security Exhibit.

b. Policies and Procedures; Training; Sanctions: 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 training on its privacy and information security policies and procedures, and no less than annually thereafter. Business Associate will provide additional training to Workforce members upon request by Sutter. Business Associate shall have a written policy regarding sanctions, and apply appropriate sanctions to its Workforce members, for unauthorized Use or Disclosure of PHI and other noncompliance with Business Associate's 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 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.

    ii. 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. 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. Upon request, Business Associate shall promptly provide Sutter with a full list of names and addresses, or other contact information, for affected Individuals, to the extent that Business Associate maintains such information.

    iii. Reports required under section shall be made by phone and in writing, by certified mail, 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 and Information Security Officer
2200 River Plaza Drive, 3rd Floor
Sacramento, CA 95833
Ph: (855) 771-4220
shpi@sutterhealth.org

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, unless it is not

readily producible in such format, in which case it shall be produced in a readable electronic format if Business Associate maintains it in an electronic format or a hard copy format if Business Associate does not maintain the information in an electronic format. If an Individual contacts Business Associate directly for such access, Business Associate shall direct the Individual to contact Sutter. This requirement to provide access to PHI shall only apply if the PHI is part of a Designated Record Set or where Sutter has an obligation under other federal or state law to provide the Individual with a copy of, or access to, their information.

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. This requirement to amend the PHI shall only apply if the PHI in Business Associate's possession is part of Sutter's Designated Record Set or where Sutter has an obligation under other federal or state law to amend the information.

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 in order for Sutter to comply with 45 C.F.R. § 164.528, as may be amended. Business Associate shall provide the information required under 45 C.F.R. § 164.528(b), including, as applicable, the date of the Disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI Disclosed, and the purpose of the Disclosure. 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). In all cases, Business Associate agrees to comply with guidance issued from time to time by the U.S. Department of Health and Human Services ("HHS") regarding the minimum necessary standard.

j. Prohibition on Sale of PHI: Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI in violation of HIPAA. 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: Business Associate shall make its written agreements, internal practices, books, documents, and records relating to the Use and Disclosure of PHI received from, or created or received by Business Associate on behalf of, Sutter available to the Secretary of HHS ("Secretary"), and/or Sutter, for purposes of determining Sutter's and/or Business Associate's compliance with this Agreement, HIPAA or other applicable laws and regulations. Business Associate shall cooperate with Sutter related to government or regulatory investigations, including reasonably anticipated investigations or inquiries, including making Business Associate's information relating to the Use and Disclosure of PHI available to Sutter. Unless prohibited, Business Associate shall immediately notify Sutter if Business Associate receives a request or notification from the Secretary or other government agency related to Sutter's compliance with applicable laws or regulations or related to Business Associate's compliance to the extent such compliance may affect or relate to PHI. This paragraph shall survive termination of this Agreement. Nothing in this section shall be construed as a waiver of any legal privilege or any protections of trade secrets or confidential commercial information.

l. Identity Theft Red Flags: To the extent Business Associate performs a service or activity on behalf of Sutter in connection with a covered account (as defined by 16 C.F.R. § 681.1(b)(3)), Business Associate will perform the service or activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft (as defined in 16 C.F.R. § 603.2(a)).

m. Payment Card Industry Data Security Standards ("PCI DSS") Compliance: To the extent Business Associate has access to or receives, stores, processes, or transmits any cardholder data or sensitive authentication data, as defined by the PCI DSS, from or on behalf of Sutter, Business Associate shall comply with the currently effective version of the PCI DSS with respect to such information. Business Associate represents and warrants that it is currently certified to be in compliance with the currently effective version of the PCI DSS. Business Associate

agrees to continue to meet all PCI DSS requirements and to validate that compliance annually according to the credit card industry rules, which include but are not limited to the PCI Security Standards Council's PCI DSS. Business Associate will provide written evidence of this compliance to Sutter upon request. If applicable, Business Associate agrees that their electronic check processing functionality will comply with the appropriate NACHA-The Electronic Payment Association provisions. Applications purchased from a third party that will be used by to store, process or transmit cardholder data must be Payment Application Best Practices (PABP) certified (This certification ensures that the application is compatible with PCI requirements).

n. Mitigation Procedures: Business Associate agrees to 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.

o. 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.

p. 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. This provision shall survive the termination or expiration of this Agreement.

q. Insurance: Business Associate 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 or payment card information, including any Use or Disclosure not permitted by this Agreement, and any Breach, loss, or compromise of any PHI or payment card information. Such insurance shall provide coverage in an amount not less than $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. Business Associate shall also ensure that any Subcontractors that create, receive, maintain, or transmit PHI or payment card information on behalf of Business Associate agree to the same insurance requirements that apply to Business Associate. Upon request, Business Associate shall furnish Certificates of Insurance to Sutter within ten (10) days of such request.

r. Legal Process: 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.

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.

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

c. Except as otherwise prohibited in this Agreement, Business Associate may Use or Disclose PHI for Business Associate's own proper management and administration, and to fulfill any of Business Associate's legal responsibilities; provided, however, that any Disclosure is Required by Law or Business Associate has received

from any third party recipient of PHI written assurances that (i) the PHI will be held confidentially and Used or further Disclosed only as Required by Law or for the purposes for which it was Disclosed to the third party, and (ii) the third party will notify Business Associate of any instances of which the third party becomes aware that the confidentiality of the PHI has been breached.

d. 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:

Sutter Health Plus
2700 Gateway Oaks Drive, Suite 1200
Sacramento, CA 95833

5. Termination**.**

a. Breach: If Business Associate breaches its obligations under this Agreement, 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, and may, but is not required to, provide Business Associate an opportunity to cure the breach within thirty (30) days prior to the effectiveness of such termination (or such shorter time period as determined by Sutter in its sole discretion). For the avoidance of doubt, no advance written notice of termination shall be required in the event of Business Associate's breach of terms of this Agreement.

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

c. Procedure upon Termination: Upon 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, and shall retain no copies of PHI, except as provided below. Business Associate will return all PHI within fourteen (14) days of the effective date of termination, unless otherwise agreed to in writing by the Parties, at no cost to Sutter. Business Associate will return such PHI in an industry-standard flat-file format, using encrypted media or encrypted transmission as agreed to by the Parties, and provide any and all passwords for such files, at no cost to Sutter. 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 the Parties agree that the 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 or Disclosure of the PHI to those purposes that make the return or destruction of the PHI infeasible for so long as Business Associate maintains the PHI. Business Associate shall notify Sutter what PHI Business Associate shall retain. This obligation on Business Associate shall survive any termination of this Agreement.

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

7. Amendment. 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.

8. Third Party Beneficiaries. Each Sutter Health Affiliate shall be deemed a third party beneficiary of this Agreement. Notwithstanding the foregoing, nothing contained herein is intended nor shall be construed to create any rights or remedies, running to the benefit of third parties.

9. 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.

10. 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 the attached exhibit, shall control.

11. 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.

12. 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.

13. 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.

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

15. Effect on Underlying Service Agreements. Except as inconsistent with this Agreement or as necessary to implement the provisions of this Agreement, all other terms in the Underlying Service Agreements shall remain in full force and effect.

16. Consent or Approval by Sutter. 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.

17. No Limitation of Liability. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT OR THE UNDERLYING SERVICE AGREEMENTS, ANY PURPORTED LIMITATION ON A PARTY'S LIABILITY, AS TO TYPE OR AMOUNT OF DAMAGES, SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF A VIOLATION OF THIS AGREEMENT, UNLESS SUBSEQUENTLY AGREED TO BY WRITTEN AMENDMENT EXECUTED BY AUTHORIZED MANAGEMENT LEVEL REPRESENTATIVES OF BOTH PARTIES.

18. 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 and Information Security Officer**	Title: .....
Date:	Date: .....

INFORMATION SECURITY EXHIBIT

Business Associate represents and warrants that it maintains industry standard information security, including, as applicable, consistent with standards set forth by the National Institute of Standards and Technology. Capitalized terms used in this Exhibit and not defined herein shall have the meaning set forth in the Business Associate Agreement. For purposes of this Exhibit, "Systems" means without limitation all computers, computer systems, networks, databases, servers, communication systems, Intranet(s) and means of access to such systems, including but not limited to, passwords, tokens, keys, logon scripts or other authentication information. Business Associate shall limit its Use and Disclosure of PHI to only as necessary and appropriate to fulfill its specific obligations to Sutter, and as permitted under the Business Associate Agreement, and shall implement administrative, physical, and technical safeguards to prevent any unauthorized Use or Disclosure of PHI. Without limiting the foregoing, Business Associate agrees to the following:

A. Administrative Safeguards

1. **Information Security Management**

   a. Risk Analysis. Business Associate will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity and Availability of PHI in accordance with HHS guidance and NIST standards. Business Associate will perform quarterly vulnerability scans on information systems creating, receiving, storing, transmitting or transacting PHI.

   b. Risk Management. Business Associate will develop and implement a risk management plan. Business Associate will evaluate, implement and maintain security measures based on an analysis of the risks. Business Associate, using reasonable and appropriate measures, will protect PHI against unauthorized (malicious or accidental) disclosure, modification, or destruction of information, unintentional errors and omissions, IT disruptions due to natural or man-made disasters, and failure to exercise due care and diligence in the implementation and operation of Business Associate's information systems. Business Associate will maintain effective controls and procedures guarding against, detecting, and reporting malicious software.

   c. Storage and Security. Business Associate shall operate and maintain the servers in good working order with access restricted to qualified employees of Business Associate. The detailed description of Business Associate's service environment shall be incorporated in this Exhibit as Appendix A. Any changes to the detailed description of Business Associate's service environment, including facility location, and applicable security requirements and controls in Appendix A must be provided to Sutter in writing at least thirty (30) days prior to such changes.

   d. Maintenance. Business Associate shall maintain all software so as to remain within one generation of the then current maintenance releases and remain on a supported release unless otherwise agreed to in writing by Sutter. This shall include, but not be limited to, the obligation to promptly implement any security-related Enhancementor Fix made available by the supplier of such software.

   e. Patches. Business Associate will apply all applicable security patches, service packs and hot fixes on applications and information systems that create, receive, transmit, transact or store PHI within thirty (30) days of release.

   f. Information System Activity Review. Business Associate will regularly capture and review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Business Associate will employ Security Event and Incident Monitoring (SEIM) technology such as intrusion detection and prevention systems on IT systems that create, receive, transmit, transact, or store PHI and will review and analyze activity records for indications of inappropriate or unusual activities daily. Business Associate will retain the activity logs for a minimum of six (6) years. Business Associate shall make such logs available to Sutter, upon request, as Sutter reasonably determines is necessary to investigate a potential unauthorized Use or Disclosure.

2. **Workforce Security**

[1] **"Enhancements"** means improvements which add features to, or otherwise improve functionality or performance of, a software product.

[2] **"Fix"** means an upgrade, update, workaround or other modifications to a software product, other than an Enhancement, which is made by or on behalf of the licensor in order to correct defects or errors in the software product.

a. Workforce Screening. Business Associate will perform a thorough background check that will include, at a minimum: Name and address verification; employment verification by previous employers; Primary Source Verification of Licensure; Verification of Highest Level Educational Credentials; social security number verification; County Criminal Search; National Criminal Record Search (CrimeSweep); OIG exclusion list; System for Award Management (SAM database); Office of Foreign Assets Control (OFAC); state debarment or exclusions lists; and drug testing for all employees permitted access to information systems that create, receive, transmit, transact or store PHI. Background checks will include married name and maiden name where appropriate.

b. Termination Procedure. Business Associate will terminate access to information systems that create, receive, transmit, transact or store PHI immediately upon termination of individual employment.

c. Authorization and Supervision. Business Associate will: (i) ensure that Workforce members have appropriate access to PHI following the principles of minimum necessary and least privilege and (ii) prevent Workforce members who do not have access to PHI from obtaining access to PHI.

3. **Information Access Management**

a. Access Authorization. Business Associate shall implement policies and procedures for granting access to PHI. Business Associate will provide secure role-based account management granting privileges utilizing the principle of least privilege. Business Associate will monitor all user accounts with administrative level access to Operating Systems and databases used to create, receive, transmit, transact or store PHI. Business Associate will restrict the ability to install software to only authorized technical support personnel.

b. Access Establishment and Modification. Business Associate will implement policies and procedures to establish, document, review, and modify a user's right to access systems that create, receive, transmit, transact or store PHI.

c. Permissions. When provided with an authorized request for new, changed or deleted access permissions, Business Associate will comply with such request within twenty-four (24) hours.

4. **Security Incident Response Plan.** Business Associate will maintain a formal incident response plan, which shall, at minimum, address detecting, analyzing, prioritizing and handling security incidents. Business Associate will review and update as appropriate its incident response plan annually. Business Associate shall document security incidents and their outcomes.

5. **Contingency Plan.** Business Associate shall establish and implement, as needed, formal contingency plans which detail strategies for response to and recovery from a broad spectrum of potential disasters that could disrupt operations and timely delivery of materials and services required pursuant to the Business Associate Agreement or Underlying Service Agreements, and in accordance with 45 C.F.R. § 164.308(a)(7), including:

a. Data Backup Plan. Business Associate will establish and maintain defined and documented procedures to create and maintain retrievable exact copies of PHI. Business Associate shall maintain independent archival and backup copies of the PHI in accordance with the same security standards provided to original, on-line copies.

b. Disaster Recovery Plan. Business Associate will establish and maintain defined and documented procedures to restore any loss of PHI.

c. Emergency Mode Operation Plan. Business Associate will establish and maintain defined and documented procedures to enable continuation of critical business processes for protection of the security of PHI while operating in emergency mode.

d. Application and Data Criticality Analysis. Business Associate will assess the relative criticality of specific applications and data in support of other contingency plan components.

e. Annual Test. Business Associate will conduct an annual test and evaluation of its business continuity plan(s).

f. Availability. Upon request, Business Associate will make its business continuity plan(s) and its annual evaluation available to Sutter for review.

B. Physical Safeguards

1. **Facility Access Controls.** Business Associate shall maintain controls and procedures to limit physical access to information systems that transmit, transact or store PHI and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed. Business Associate shall maintain controls and procedures to validate personnel access to facilities based on their role, including visitor controls.
2. **Workstation Use.** Business Associate shall maintain controls and procedures specifying the secure configuration of workstations having access to information systems that transmit, transact or store PHI.
3. **Workstation Security.** Business Associate will implement physical safeguards for all workstations that access, create, receive, transmit, transact, or store PHI to restrict access to authorized users.
4. **Device and Media Controls.** Business Associate shall implement controls and procedures that govern the receipt and removal of hardware and electronic media that create, receive, transmit, transact, or store PHI into and out of a facility (including but not limited to an inventory of all such hardware and electronic media), and the movement of these items within the facility.
5. **Disposal and Media Re-use.** Business Associate will securely sanitize all media used to create, receive, transmit, transact, or store PHI in accordance with HHS Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, as may be updated from time to time, and in accordance with NIST Special Publication 800-88 Guidelines for Media Sanitization, as may be updated from time to time, prior to disposal or re-use of any such media or device.

C. Technical Safeguards

1. **Access Control.** Business Associate shall implement controls and procedures for information systems that create, receive, transmit, transact, or store PHI to allow access only to those persons or software programs that have been granted access rights.
2. **Unique User Identification**. Business Associate will assign a unique user ID and password for identifying and tracking user identity and will not allow the use of shared accounts.
3. **Encryption**. Business Associate will encrypt all PHI that is created, received, transmitted, transacted or stored:
   a. For data at rest, consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
   b. For data in motion, consistent with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or encryption algorithm which are Federal Information Processing Standards (FIPS) 140-2 validated.
4. **Automatic Log-off**. Business Associate will ensure that information systems that create, receive, transmit, transact, or store PHI automatically terminate or lock after fifteen (15) minutes of inactivity requiring user re-authentication.
5. **Person or Entity Authentication.** Business Associate will maintain controls and procedures to verify that a person or entity seeking access to information systems that create, receive, transmit, transact, or store PHI is the one claimed. Business Associate will employ authentication for network system access that is NIST Special Publication 800-63 compliant for Level 2 or higher. Business Associate will employ multifactor authentication (e.g., tokens, one (1) time passwords, etc.), compliant with NIST Special Publication 800-63 for Level 3 or higher, for remote access to its network (e.g., VPN access) and for all remote access to applications and information systems that create, receive, transmit, transact or store PHI.
6. **Boundary Protection.** Business Associate will monitor and control communications at the external boundary of its information systems and at key internal boundaries within the systems (e.g., firewall between internet facing servers and the internal network).

D. Audits**.** Notwithstanding any other audit provisions in the Business Associate Agreement or Underlying Service Agreements, with regard to information security, Sutter reserves the right to audit, inspect, and make copies or extracts of Business Associate's records and processes associated with Business Associate's performance under this Exhibit at any time with twenty-four (24) hours prior notice to Business Associate. Any audit or inspection will occur during Business Associate's normal business hours. Sutter's right to audit, inspect, and make copies or extracts of Business Associate's records and processes shall continue for a period of six (6) years following the termination or expiration of the Business Associate Agreement. Business Associate shall cooperate in all audits and inspections

conducted by Sutter and shall remedy any discrepancies identified pursuant to such audits and inspections within a mutually agreeable timeframe. Any audits or inspections conducted by Sutter pursuant to this Section shall in no way be deemed to relieve Business Associate of any of its obligations, responsibilities or liabilities under this Exhibit, the Business Associate Agreement, Underlying Service Agreements, or under any applicable laws. Any election by Sutter to conduct, or any failure by Sutter to conduct, any audit or inspection shall in no event be deemed to constitute Sutter's approval of any activity undertaken by Business Associate or of any method, system or procedure used by Business Associate in performance of this Exhibit, the Business Associate Agreement or Underlying Service Agreements.

E. Access to Information Systems**.** Access, if any, to Sutter's information systems is granted solely to perform the services under the Underlying Services Agreement and in accordance with the Business Associate Agreement, and is limited to those specific Sutter information systems, time periods and personnel as are separately agreed to by Sutter and Business Associate from time to time. Sutter may require Business Associate's employees, Subcontractors or agents to sign individual agreements prior to accessing Sutter's information systems. Use of Sutter's information systems during other time periods or by individuals not authorized by Sutter is expressly prohibited. Access is subject to Sutter business control and privacy and information security policies, standards and guidelines as may be modified from time to time. Use of any other Sutter information systems is expressly prohibited. This prohibition applies even when a Sutter information systems that Business Associate is authorized to access serves as a gateway to other information systems outside Business Associate's scope of authorization. Business Associate agrees to access Sutter's information systems only from specific locations approved for access by Sutter. For access outside of Sutter premises, Sutter will designate the specific network connections to be used to access Sutter's information systems.