Business Associate Agreement Instructions

Executive Sponsor or his/her designee is responsible for reviewing Business Associate Agreements Policy and Procedure in Policy and Procedure Manager (PPM).

Per policy, Business Associate Agreements (BAA) are not permitted to be executed until an Information Security Third Party Risk Assessment has been completed.

Instructions

1. Remove these instructions from the template
2. Send the attached BAA template to the vendor to review and approve
    a. Edits/changes by the vendor need to be sent to Legal Affairs (GroupLegalAffairsBAA@cshs.org)
3. Submit a request for an Information Security Third Party Risk Assessment in Service Center
4. Once the risk assessment is completed, complete the business agreement process and attach the BAA

Questions about the Business Associate Agreement Policy & Procedures, contact Corporate Integrity (CorporateCompliance@cshs.org)

Exhibit "__"
Business Associate Agreement

This Exhibit constitutes the Business Associate Agreement ("Agreement") between Cedars-Sinai and all of its affiliates (collectively "Covered Entity"), and the contractor, vendor or other party to the contract to which this Exhibit is attached (the "Business Associate").

RECITALS

WHEREAS, Business Associate provides services ("Services") to Covered Entity, and Business Associate receives, and may have access to or create Protected Personal Health Information (as defined below) in order to provide those Services;

WHEREAS, Covered Entity and Business Associate are subject to the requirements of the Health Insurance Portability and Accountability Act of 1996, as amended from time to time, including the amendments and related laws of the Health Information Technology for Economic and Clinical Health Act, and regulations promulgated thereunder, including but not limited to the "Privacy Rule" (45 C.F.R. Part 160 and Subparts A and E) and the "Security Rule" (45 CFR Parts 160 and Subparts A and C of Part 164), California laws relating to the privacy of patient and individual information and other applicable laws, and 42 C.F.R. Part 2, to the extent applicable ("HIPAA/Federal/State Privacy Laws");

WHEREAS, HIPAA/Federal/State Privacy Laws require Covered Entity to enter into a contract with Business Associate in order to mandate certain protections for the privacy and security of Protected Personal Health Information and the parties intend that this Agreement constitute, among other things, a Business Associate Agreement under federal law;

NOW, THEREFORE, in consideration of the foregoing, and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

ARTICLE I
EFFECTIVE DATE

This Agreement is effective as of the date Business Associate first receives, accesses, transmits, or creates Protected Personal Health Information under the Service(s) Agreements (the "Effective Date"). If Covered Entity and Business Associate have previously entered into a Business Associate Agreement, this Agreement supersedes such prior Business Associate Agreement from and after the Effective Date.

ARTICLE II
DEFINITIONS

2.1 "Disclose" and "Disclosure" mean, with respect to Protected Personal Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Personal Health Information.

2.2 "Information System" means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

2.3 "Protected Personal Health Information" means information derived from the Covered Entity's activities or Business Associate's activities on behalf of the Covered Entity, whether oral or recorded in any form or medium that (i) relates to the past, present or future physical or mental health or 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 and identifies the individual (or for which there is a reasonable basis for believing that

the information can be used to identify the individual); or (ii) constitutes other personal information consisting of an individual's first name or first initial and last name in combination with any of the following: (a) social security number, (b) driver's license number or identification number, (c) account number or credit or debit card number, in combination with any required security code, an access code, (d) address, (e) medical or health insurance information, or (f) information collected through the use or operation of an automated license plate recognition system. "Protected Personal Health Information" shall at all times include, without limitation, the meaning of Protected Health Information or Electronic Protected Health Information under HIPAA/Federal/State Privacy Laws.

2.4 "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information in, or interference with system operations of, an Information System which contains Protected Personal Health Information. However, Security Incident does not include attempts to access an Information System when those attempts are not reasonably considered by Business Associate to constitute an actual threat to the Information System.

2.5 "Services Agreement(s)" mean any and all contracts between the Covered Entity and any of its affiliates and Business Associate.

2.6 "Use" or "Uses" mean, with respect to Protected Personal Health Information, the sharing, employment, application, utilization, examination or analysis of such information within Business Associate's internal operations.

ARTICLE III
SPECIFIC OBLIGATIONS OF BUSINESS ASSOCIATE

3.1 Permitted Uses and Disclosures of Protected Personal Health Information. Business Associate shall neither permit the unauthorized or unlawful access to, nor use or disclosure of, Protected Personal Health Information other than as permitted or required by the Services Agreement, this Agreement, or as required by law. Except as otherwise limited in the Services Agreement, this Agreement, or the Privacy Rule or Security Rule, Business Associate may access, use, or disclose Protected Personal Health Information (i) to perform its Services as specified in this Agreement and the Services Agreement(s); and (ii) for the proper management and administration of Business Associate, including carrying out its legal responsibilities, provided that such access, use, or disclosure would not violate HIPAA/Federal/State Privacy Laws if done or maintained by Covered Entity. If Business Associate discloses Protected Personal Health Information to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable assurances from such third party that such Protected Personal Health Information will be held confidential as provided pursuant to this Agreement and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) agreement from such third party to promptly notify Business Associate of any breaches of confidentiality or security of the Protected Personal Health Information, to the extent it has obtained knowledge of such breach.

3.2 Aggregation and De-Identification of Data. For the avoidance of doubt, Business Associate may only perform data aggregation and/or de-identify Protected Personal Health Information if required to perform its Services to Covered Entity or such use is specifically authorized in writing by the Covered Entity. Business Associate, and its agents, shall request, Use and Disclose only the minimum amount of Protected Personal Health Information necessary to accomplish the purpose of the request, Use or Disclosure and only as permitted by this Agreement or applicable HIPAA/Federal/State Privacy Laws. Business Associate shall comply

with any guidance issued by Secretary of the U.S. Department of Health and Human Services regarding compliance with the minimum necessary standard.

3.3 No Other Use or Disclosure Permitted. Business Associate shall not Use or Disclose Protected Personal Health Information for any purpose
other than as specifically permitted by this Agreement or required by law. To the extent that the disclosure is not permitted by 42 C.F.R. Part 2, Business Associate will resist, in judicial proceedings if necessary, any efforts to obtain the Protected Personal Health Information.

3.4 Adequate Safeguards for Protected Personal Health Information. Business Associate warrants that it shall comply with the Security Rule and implement and maintain appropriate safeguards to prevent the Use or Disclosure of Protected Personal Health Information in any manner other than as permitted by this Agreement. Business Associate warrants that it shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Protected Personal Health Information, including limiting the incidental Uses or Disclosures that result from Uses and Disclosures permitted under this Agreement. Business Associate shall provide any information reasonably requested by Covered Entity to verify such safeguards are in place.

3.5 Risk Assessment and Audit/Ongoing Security Commitments. Business Associate shall cooperate with Covered Entity in completing all facets of the required security risk assessment. Further, Business Associate must comply with any agreed upon remediation or mitigation of security issues identified during the risk assessment.

3.6 Reporting Non-Permitted Use or Disclosure and Security Incidents. Business Associate shall report to Covered Entity each Use or Disclosure that is made by Business Associate, its employees, representatives, agents or subcontractors which is not specifically permitted by this Agreement, as well as each Security Incident of which Business Associate becomes aware and any information breach reportable under HIPAA/Federal/State Privacy Laws (each a "Reportable Incident"). The initial report shall be made by telephone call to the Covered Entity's Executive Director, Health Information at (323) 866-7840 within twenty-four (24) hours from the time the Business Associate becomes aware of the Reportable Incident, followed by a detailed written report to the Privacy Officer sent by encrypted email to GroupHIPAAPrivacy@cshs.org no later than five (5) business days from the date the Business Associate becomes aware of the Reportable Incident. Business Associate shall thereafter keep the Covered Entity's Executive Director, Health Information informed in a timely manner of all additional information obtained or developed by Business Associate with regard to any matter reportable to the Covered Entity pursuant to this Section. Business Associate will not notify patients or other third parties, such as regulatory agencies, of a breach of unsecured Protected Personal Health Information without obtaining written approval from the Covered Entity's Executive Director, Health Information.

3.7 Cooperation/Mitigation of Harmful Effect. Business Associate agrees to cooperate with Covered Entity with regard to the investigation and mitigation of any breach relating to Business Associate's Services or activities under this Agreement or any Agreement with Covered Entity. Business Associate specifically agrees, at its cost, to promptly mitigate any harmful effect of a Use or Disclosure of Protected Personal Health Information by Business Associate or Business Associate's agents in violation of the requirements of this Agreement, including the cost of credit monitoring if Covered Entity reasonably determines that there is a risk of identity theft. All such efforts shall be subject to the Covered Entity's prior written approval.

3.8 Access to and Amendment of Protected Personal Health Information. Business Associate shall, to the extent Covered Entity determines that any Protected Personal Health Information that may be retained by Business Associate constitutes a "designated record set" under HIPAA/Federal/State Privacy Laws or medical record in accordance with Covered Entity's policies, (a) make Protected Personal Health Information specified by Covered Entity available to patient or other individual(s) identified by Covered Entity, and (b) make any amendments to Protected Personal Health Information that are requested by Covered Entity. Business Associate shall provide such access and make such amendments within the time and in the manner specified by Covered Entity. If any patient requests an amendment of Protected Personal Health Information directly from Business Associate or its agent, Business Associate shall notify Covered Entity in writing within five (5) days of the request. Any approval or denial of amendment to Protected Personal Health Information maintained by Business Associate or its agent shall be the responsibility of Covered Entity. For the avoidance of doubt, Business Associate understands and acknowledges that Business Associate is required to provide Covered Entity with access to Protected Personal Health Information under this section until this Agreement is terminated, regardless of any dispute that may exist between the parties.

3.9 Accounting of Disclosures. Within ten (10) business days of any request of Covered Entity, Business Associate shall provide to Covered Entity an accounting of each Disclosure of Protected Personal Health Information made by Business Associate or its employees, agents, representatives or subcontractors to enable Covered Entity to fulfill its obligations under the Privacy Rule. Any accounting provided by Business Associate under this Section shall comply with the requirements of 45 C.F.R. §164.528. In the event that the request for an accounting is delivered directly to Business Associate or its agent, Business Associate shall within five (5) days of a request forward it to Covered Entity in writing. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested.

3.10 Business Associate's Subcontractors. Business Associate shall ensure that any agents, including subcontractors, who create, receive, maintain or transmit Protected Personal Health Information covered by this Agreement on behalf of Business Associate or Covered Entity, agree in writing to substantially similar but no less restrictive restrictions, conditions, and obligations that apply to Business Associate with regard to Protected Personal Health Information as set forth in this Agreement.

3.11 Breach of this Agreement. Any breach of this Agreement shall constitute a material breach of each of the other Agreements with Covered Entity. Covered Entity shall have the right to terminate this Agreement on written notice to Business Associate in the event Business Associate breaches this Agreement, which termination may be immediate or effective at such other time determined by the Covered Entity.

3.12 Business Associate's Performance of Covered Entity's Regulatory Obligations. To the extent Business Associate and Covered Entity have agreed that Business Associate will perform one or more of Covered Entity's regulatory obligations under the federal Privacy Rule, Subpart E of 45 C.F.R. Part 164, such as the obligation to deliver Notices of Privacy Practices to patients, Business Associate agrees to comply with the requirements of Subpart E and any other privacy laws protecting Protected Personal Health Information applicable to Covered Entity in the performance of such obligation(s).

ARTICLE IV
TERM AND TERMINATION

4.1 Term and Termination. The term of this Agreement shall be effective as of the Effective Date and shall terminate when all Protected

Personal Health Information 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.

4.2 Disposition of Protected Personal Health Information Upon Termination or Expiration. Upon termination or expiration of all Services Agreements between the parties, Business Associate shall either return or destroy, in Covered Entity's sole discretion and in accordance with any instructions by Covered Entity, all Protected Personal Health Information in the possession or control of Business Associate or its agents and subcontractors. However, if Business Associate determines that neither return nor destruction of Protected Personal Health Information is feasible and notifies Covered Entity in writing of that determination, Business Associate may retain Protected Personal Health Information provided that Business Associate (a) continues to comply with the provisions of this Agreement for as long as it retains Protected Personal Health Information, and (b) further limits Uses and Disclosures of Protected Personal Health Information to those purposes that make its return or destruction infeasible.

ARTICLE V
INDEMNIFICATION

Business Associate shall indemnify, defend and hold Covered Entity harmless from and against any claim, cost or liability arising out of the actions or inactions of Business Associate or agents or employees, or the breach by Business Associate of this Agreement.

ARTICLE VI
MISCELLANEOUS TERMS

6.1 Access to Records. Business Associate shall make its internal practices, books and records relating to the Use and Disclosure of Protected Personal Health Information available to Covered Entity and to the Secretary of the U.S. Department of Health and Human Services for the purposes of determining the parties' compliance with HIPAA/Federal/State Privacy Laws. Business Associate shall concurrently provide Covered Entity with a copy of any Protected Personal Health Information that Business Associate provides pursuant to any governmental inquiry.

6.2 Relationship to Agreements with Covered Entity and Prior Business Associate Agreements. In the event that a provision of this Agreement is contrary to a provision of any Agreement with Covered Entity pertaining to Business Associate's Services or any prior Business Associate Agreement between the parties, the provisions of this Agreement shall control.

6.3 Additional Parties - Third Party Beneficiaries. There are no third party beneficiaries to this Agreement. To the extent an affiliate of Covered Entity shares Protected Personal Health Information with Business Associate, this Agreement shall also apply to Business Associate's services for such affiliate.

6.4 No Agency. Each party shall be deemed to be an independent contractor and not an agent, joint- venturer or representative of the other party, and neither party may create any obligations or responsibilities on behalf of or in the name of the other party.

6.5 Ownership of Information. As between the parties, Covered Entity holds all right, title, and interest in and to the Protected Personal Health Information and information derived therefrom, unless otherwise agreed by the parties in writing.

6.6 Assignment. The parties may assign this Agreement in the event of a sale or merger of Business Associate upon thirty (30) days' prior written notice to Covered Entity. Covered Entity may, at its election, terminate this Agreement and the Services Agreement(s) upon receipt of such notice. Any assignment provision in the Services Agreement shall not apply if it conflicts with this section.

6.7 Compliance with Applicable Law. Business Associate agrees to comply with all applicable provisions of HIPAA/Federal/State Privacy Laws. If not otherwise specifically set forth in this Agreement, all provisions of HIPAA/Federal/State Privacy Laws are specifically incorporated into this Agreement.

6.8 Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of applicable law. Any amendments that are limited solely to provisions specifically required by law or regulation may be added by Covered Entity upon thirty (30) days' prior written notice.

Version: 2020-10-12