The purpose of this policy is to set forth the requirements necessary to document the University’s efforts to assure that business associates, agents and subcontractors comply with the HIPAA privacy and security standards and that the University knows of and has the opportunity to take remedial action regarding any breach of which it becomes aware caused by a Business Associate.

A covered entity is required to assure, to the extent practical, that any business associate with whom it shares protected health information (PHI) handles that information in accordance with the privacy & security regulations. The purpose of this policy is to set forth the requirements necessary to document the University’s efforts to assure that business associates, agents and subcontractors comply with the HIPAA privacy and security standards and that the University knows of and has the opportunity to take remedial action regarding any breach of which it becomes aware caused by a Business Associate.

II. Definitions:

**Accounting of Disclosures**: A record of all disclosures of PHI, within the prior six years, to outside parties, except those made for purposes of Treatment, Payment, and Healthcare Operations (TPO) or with a patient’s Authorization that a covered entity must give a patient at their request. This would include disclosures made during a research protocol conducted under a Waiver, to, e.g., sponsors, Business Associates and governmental agencies.

**Business Associates (BA)**: A person or entity that has access to protected health information (PHI) as a result of providing services to or for a covered entity. Specifically, on behalf of a covered entity in which the function or activity involves the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or re-pricing, legal, actuarial, consulting data aggregation, management, management, administrative, accreditation,
software support requiring routine access to PHI, financial and/or accounting services. Business Associates also include Patient Safety Organizations and Health Information Exchanges (HIE's).

**Business Associate Agreement**: Legal written contract between a third party and a covered entity, which specifies the permitted uses and disclosures and safeguards for protected health information (PHI).

**Covered Entity (CE)**: The covered entity refers to healthcare providers, health plans and healthcare clearinghouses that perform a covered service and transmit data electronically and must comply with HIPAA.

**Disclosure**: The release, transfer or provision of access to, or divulging in any other manner of information outside of the entity holding the information. [164.501]

**Protected Health Information (PHI)**: Any individually identifiable health information collected or created as a consequence of the provision of health care by a covered entity in any form, including verbal communications with a staff member. Records covered by FERPA are excluded.

**Provider**: Any person or entity supplying medical services and who bills for or is paid for medical services “in the normal course of business.”

**Use**: The sharing, employment, application, utilization, examination or analysis of such information with the entity that maintains such information.

### III. Policy Text:

A. It is the policy of UCR Health that use and disclosure of protected health information (PHI) may only be shared with business associates when an approved written business associate agreement (BAA) is in force to safeguard the PHI. BAA's must be in writing and must contain the UC system-wide approved BAA language and authorized signatures. Any changes to the UC System-wide approved language must be approved by the UCR Compliance and Privacy Officer, Purchasing Officer, Campus Legal Counsel, and the UCR Risk Manager.

B. UCR may disclose PHI to a business associate and may allow that business associate (BA) to create or receive PHI for or on behalf of UCR, if UCR and the business associate enter into a written business associate agreement (“BAA”). UCR is not required to enter into a business associate agreement (“BAA”) with other treating health care provider(s) prior to disclosing PHI or other information related to treatment of an individual.

C. At any time that the University determines that a business associate has violated a material term or obligation of the agreement relating to HIPAA compliance, the department that is party to the agreement and the Compliance and Privacy Officer shall be notified and shall seek to immediately remedy the breach.

D. The Compliance and Privacy Officer will also notify the University of California Senior Vice President for Ethics and Compliance to notify him/her of the breach as the Business Associate may be providing services at more than one UC campus.

E. If it is not possible to remedy the breach, UCR Health and/or the University will move to terminate the agreement. Violations may also be reported by UCR to the Secretary of the Department of Health & Human Services.

F. It is the responsibility of each UCR School of Medicine department, division, or operating unit contracting for services with third parties to whom identifiable health information will be shared, to assure that valid business associate agreements are executed prior to the disclosure of any protected health information (PHI).
IV. Responsibilities:
   A. All Health Sciences Personnel
      1. Department / Division Responsibility
      2. The Purchasing Office
      3. Responsibilities of the Business Associate
   B. Director of Purchasing at UC Riverside
      1. Secretary of JHHS
      2. Return or Destroy PHI
      3. Breach Notification
      4. Service/Purchasing/Affiliation
      5. Accounting for Disclosures
      6. Reporting Violations
      7. Record Retention
   C. Compliance and Privacy Office
      1. Exceptions that Do Not Require a Business Associate Agreement

V. Procedures:
   A. Department / Division Responsibility
      1. It is the responsibility UCR School of Medicine departments, divisions, or operating
         units contracting for services with third parties to whom identifiable health
         information will be shared, to assure that valid business associate agreements are
         executed. However the BAA must be signed by UCR Campus Purchasing Officer,
         who has the delegated responsibility to sign the Business Associate agreement on
         behalf of the University of California.
   B. The Purchasing Office can also be requested to check the system-wide database to
determine if a System-wide Business Associate agreement is currently in place with the
Business Associate.
   C. Arrangements that are unclear as to status must be referred to the Purchasing Director
or Compliance and Privacy Officer for further determination. UCR has no obligation to
monitor the activities/practices of the BA, but UCR may request or ask these types of
questions, as an option, if assurances are desired, e.g.
      1. Copy of the BA’s current security and privacy policies as an exhibit to the business
         associate agreement; or
      2. Do you have written agreements with every subcontractor who processes PHI for
         you in which the subcontractor agrees to protect the integrity and confidentiality of
data exchanged between you?
      3. Do you have a contingency plan in place that provides for a
         a. One year data back-up plan
         b. Disaster recovery plan
         c. Emergency mode of operation plan?
      4. Do you have written policies and procedures establishing rules for granting access
to protected health information?
   D. Responsibilities of the Business Associate: The business associate agreement
sets forth the actions for which the business associate will be responsible, including:
      1. Permitted Uses of PHI: The BA may only use or disclose PHI as permitted by the
         contract or agreement describing the services provided to the CE or as required by
         law.
      2. Safeguards: The BA must use appropriate safeguards to protect the confidentiality
         of the information and to prevent use or disclosure other than as provided in the
         contract.
3. **Reporting to the Covered Entity:** The BA must report to the CE any use or disclosure not permitted for by the contract of which the BA becomes aware.

4. **Obligations of Subcontractors:** The BA must ensure that any subcontractor or agent to which it provides PHI adheres to the same restrictions and conditions that apply to the BA, and that all subcontractors are provided education on the BAA’s policies.

5. **Patient Access to PHI:** The BA must make PHI available to the CE or a patient (upon individual request as appropriate) any information necessary for the CE to comply with the patients’ rights to access, amend and receive an accounting of disclosures of their PHI.

6. **Secretary of DHHS:** The BA must make available upon request to the Secretary of the Department of Health & Human Services (DHHS) the business associate’s internal practices, books and records relating to the use and disclosure of PHI.

7. **Return or Destroy PHI:** Once the contract is terminated, return or destroy the information, if feasible. If it is not possible to return or destroy the information because of other obligations or legal requirements, the protections of the agreement must apply until the information is returned or destroyed, and no other uses or disclosures may be made except for the purposes that prevented the return or destruction of the information.

8. **Breach Notification:** The Business Associate is required to notify the University if it discovers or suspects that a breach of patient information has occurred.

9. **Exceptions that Do Not Require a Business Associate Agreement:** The following exceptions do not require a BAA:
   1. Disclosure of PHI is for treatment purposes;
   2. Disclosures for financial transactions, e.g., bank or credit card transactions;
   3. Disclosures between group health plans and plan sponsor;
   4. Disclosures between the covered entity’s (CE) workforce members for treatment, payment and health care operations (TPO);
   5. Disclosures to other CE’s for purposes of TPO;
   6. Disclosures to other contracted individuals and volunteers or trainees if they function as a member of the CE’s workforce and receive privacy training.

10. **Service / Purchase / Affiliation Agreements:** The designated purchasing staff members will review all existing and future purchase agreements, service agreements and other healthcare business, teaching / training, and care relationships (e.g., affiliation agreements) to identify which agreements will require the additional business associate agreement and will incorporate the terms of the BAA by specific reference to the BAA. See Appendix B for decision tree to determine if a Business Associate Agreement is needed.

11. **Questions and Communications:** Communication regarding confidentiality and privacy policies and monitoring shall be channeled through the UCR Health Compliance and Privacy Officer (951-827-4672).

12. **Accounting for Disclosures:** Ordinarily disclosures of PHI to a BA used under a BAA need not be included in the accounting; however, disclosures of PHI for non-permitted uses must be logged and made available to the patient upon request.

13. **Reporting Violations:** All known or suspected violations of this policy should be reported to the Compliance and Privacy Officer or to Human Resources by any person having knowledge of the violation or to the UCR Confidential Compliance Message Line (1-800-403-4744).
N. Record Retention: A copy of the BAA, executed by UCR and the Business Associate, must be stored by UCR for a period of six years after the BAA is no longer in effect, e.g., in UCR's "Business Associate Agreement" file.

VI. Forms/Instructions:
   A. Appendix A: UC System-Wide Business Associate Agreement
   B. Appendix B: Decision Tree

VII. Contacts:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Title</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Compliance and Privacy Officer</td>
<td>(951) 827-4672</td>
</tr>
<tr>
<td>Compliance</td>
<td>Privacy Analyst</td>
<td>(951) 827-7672</td>
</tr>
<tr>
<td>Purchasing</td>
<td>Purchasing Director</td>
<td>(951) 827-3009</td>
</tr>
</tbody>
</table>

Viii. Revision History: N/A

Approval(s)

James R. Herron  
Compliance and Privacy Officer  
School of Medicine
Appendix A

HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement ("BA AGREEMENT") supplements and is made a part of any and all agreements entered into by and between The Regents of the University of California, a California corporation ("UNIVERSITY"), on behalf of its University of California Health System and _____________________ ("BUSINESS ASSOCIATE") and is effective as of ___________________ ("Effective Date"). UNIVERSITY has designated all of its HIPAA health care components as a single component of its hybrid entity and therefore this agreement is binding on all other health care components of the UNIVERSITY.

RECITALS

A. UNIVERSITY and BUSINESS ASSOCIATE desire to protect the privacy and provide for the security of Protected Health Information (as that term is defined herein) used by or disclosed to BUSINESS ASSOCIATE in compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the regulations promulgated thereunder by the U.S. Department of Health and Human Services (45 CFR Parts 160, 162 and 164, the "HIPAA Regulations"), the Health Information Technology for Economic and Clinical Health Act of 2000 (the "HITECH Act"), California Health and Safety Code §§1280.15, California Civil Code §§1798.82 and 1798.29, and other applicable laws and regulations. The purpose of this BA AGREEMENT is to satisfy certain standards and requirements of HIPAA, the HIPAA Regulations, including 45 CFR § 164.504(e), and the HITECH Act, including Subtitle D, part 1, as they may be amended from time to time.

B. BUSINESS ASSOCIATE provides services to UNIVERSITY, or performs or assists in the performance of UNIVERSITY activities or functions, involving the use or disclosure of Protected Health Information in the course of such service or assistance.

C. UNIVERSITY wishes to disclose to BUSINESS ASSOCIATE certain information, some of which may constitute Protected Health Information or Medical Information (herein collectively referred to as "PHI").

Therefore, intending to be legally bound hereby, the parties agree as follows:

1. EFFECT OF AGREEMENT. This BA AGREEMENT amends, supplements and is made a part of any and all agreements between UNIVERSITY and BUSINESS ASSOCIATE, regardless of whether the agreement(s) shall have been entered into before or after the Effective Date of this BA AGREEMENT. To the extent that the terms of the agreement(s) are inconsistent with the terms of this BA AGREEMENT, the terms of this BA AGREEMENT shall control.

2. DEFINITIONS.

2.1 "Breach" means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such
information, and shall have the meaning given to such term under HIPAA and the HIPAA regulations, including 45 CFR §164.402, as well as California Civil Code §§ 1798.29 and 1798.82.

2.2 “Electronic Health Record” means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given to such term under the HITECH Act, including Section 13400(3).

2.3 “Electronic PHI” means PHI that is transmitted by or maintained in electronic media and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 160.103. For the purposes of this BA AGREEMENT, Electronic PHI includes all computerized data, as defined in California Civil Code §§ 1798.29 and 1798.82.

2.4 "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, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.304.

2.5 "Medical Information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment and shall have the meaning given to such term under California Civil Code § 56.05.

2.6 "Protected Health Information" ("PHI") means any information, including Electronic PHI, 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, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including, but not limited to 45 CFR § 160.103. For the purposes of this BA AGREEMENT, PHI includes all medical information and health insurance information as defined in California Civil Code §§ 56.05 and 1798.82.

2.7 "Secretary" means the Secretary, Department of Health and Human Services, or his or her designee.

2.8 "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.304.

2.9 "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of an Encryption or Destruction technology or methodology specified by the Secretary in guidance issued under Section 13402(h)(2) of the HITECH Act on the Health and Human Services Web site, as such guidance may be revised from time to time, and shall have the meaning given to such term under HIPAA
and the HIPAA Regulations, including 45 CFR § 164.402.

2.9.1 “Encryption” means a technology or methodology that utilizes an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key, and such confidential process or key that might enable decryption has not been breached, and shall have the meaning given to such term under HIPAA and HIPAA Regulations, including 45 CFR § 164.304.

2.9.2 “Destruction” means the use of a technology or methodology by which the media on which the PHI is stored or recorded has been shredded, destroyed, cleared, or purged, as appropriate, such that the PHI cannot be read, retrieved, or otherwise reconstructed. Redaction is inadequate for the purposes of destruction.

3. RESPONSIBILITIES OF BUSINESS ASSOCIATE.

3.1 Permitted Uses and Disclosures of PHI. BUSINESS ASSOCIATE may use, access, and/or disclose PHI received by BUSINESS ASSOCIATE solely for the purpose of performing a function or activity for or on behalf of the University. To the extent the BUSINESS ASSOCIATE carries out one or more of UNIVERSITY’s obligation(s) under Subpart E of 45 CFR Part 164, BUSINESS ASSOCIATE must comply with the requirements of Subpart E that apply to the UNIVERSITY in the performance of such obligation(s).

3.1.1 Minimum Necessary. With respect to the use, access, or disclosure of PHI by BUSINESS ASSOCIATE as permitted under section 3.1, BUSINESS ASSOCIATE shall limit such use, access, or disclosure, to the extent practicable, to the minimum necessary to accomplish the intended purpose of such use, access, or disclosure. BUSINESS ASSOCIATE shall determine what constitutes the minimum necessary to accomplish the intended purpose in accordance with HIPAA, HIPAA Regulations and any applicable guidance issued by the Secretary.

3.1.2 Documentation of Disclosures. With respect to any disclosures of PHI by BUSINESS ASSOCIATE as permitted under section 3.1, BUSINESS ASSOCIATE shall document such disclosures including, but not limited to, the date of the disclosure, the name and, if known, the address of the recipient of the disclosure, a brief description of the PHI disclosed, and the purpose of the disclosure.

3.1.3 Modification of PHI. Except as permitted under section 3.10.2 below, BUSINESS ASSOCIATE shall not modify any existing data to which it is granted access other than to correct errors, or derive new data from such existing data. BUSINESS ASSOCIATE shall record any modification of data and retain such record for a period of seven (7) years.

3.1.4 Electronic Transaction Standards. Where applicable, BUSINESS ASSOCIATE shall adhere to the transaction standards as specified in 45 CFR §§ Parts 160 and 162.

3.2 Other Permitted Uses and Disclosures of PHI. BUSINESS ASSOCIATE may, if necessary and only to the extent necessary, use PHI (i) for the proper management and administration of BUSINESS ASSOCIATE’s business, (ii) to provide data aggregation services relating to the health care operations of UNIVERSITY, or (iii) to carry out BUSINESS ASSOCIATE’s legal responsibilities, subject to the limitation in section 3.3, below. BUSINESS
ASSOCIATE shall obtain reasonable assurances from the person to whom the PHI is being disclosed that, as required under this BA AGREEMENT, the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed. BUSINESS ASSOCIATE shall require that any Breaches or Security Incidents be immediately reported to BUSINESS ASSOCIATE. BUSINESS ASSOCIATE shall then report the Breach or Security Incident to UNIVERSITY in accordance with section 3.7.

3.3 Nondisclosure of PHI. BUSINESS ASSOCIATE is not authorized and shall not use or further disclose UNIVERSITY’s PHI other than as permitted or required under any agreement it has with University, including this BA AGREEMENT, or as required by law or regulation.

3.3.1 Disclosures Required by Law. In the event BUSINESS ASSOCIATE is required by law to disclose PHI, BUSINESS ASSOCIATE shall promptly notify UNIVERSITY of such requirement. BUSINESS ASSOCIATE shall give UNIVERSITY sufficient opportunity to oppose such disclosure or take other appropriate action before BUSINESS ASSOCIATE discloses the PHI.

3.3.2 Legal Process. In the event BUSINESS ASSOCIATE is served with legal process or a request from a governmental agency that may potentially require the disclosure of PHI, BUSINESS ASSOCIATE shall promptly, and in any case within two (2) business days of its receipt of such legal process or request, notify UNIVERSITY. BUSINESS ASSOCIATE shall not disclose the PHI without UNIVERSITY’S consent unless pursuant to a valid and specific court order or to comply with a requirement for review of documents by a governmental regulatory agency under its statutory or regulatory authority to regulate the activities of either party.

3.4 Prohibition on Sale of PHI for Remuneration. Subject to the limitations set forth in Section 13405(d)(2) of the HITECH Act, BUSINESS ASSOCIATE shall not directly or indirectly receive remuneration in exchange for any of UNIVERSITY’s PHI unless BUSINESS ASSOCIATE first obtains authorization from UNIVERSITY. UNIVERSITY shall not grant such authorization unless the subject of the PHI has granted UNIVERSITY a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the individual’s PHI.

3.5 Security Standards. BUSINESS ASSOCIATE shall take appropriate security measures (i) to protect the confidentiality, integrity and availability of UNIVERSITY’s Electronic PHI information that it creates receives, maintains, or transmits on behalf of the UNIVERSITY and (ii) to prevent any use or disclosure of UNIVERSITY’s PHI other than as provided by the Agreement and this BA AGREEMENT. Appropriate security measures include the implementation of the administrative, physical and technical safeguards specified in Subpart C of 45 CFR Part 164 of the HIPAA Security Rule.

3.6 Security Documentation. BUSINESS ASSOCIATE shall maintain the policies and procedures implemented to comply with section 3.5 in written form (paper or electronic). If an action, activity or assessment is required to be documented, BUSINESS ASSOCIATE shall maintain a written record (paper or electronic) of the action, activity, or assessment, shall retain the documentation for six (6) years from the date of its creation or the date when it last was in effect, whichever is later, make documentation available to those persons responsible for implementing the procedures to which the documentation pertains, and review documentation periodically, and update as needed, in response to environmental or operational changes.
affecting the security of the PHI.

3.7 Notification of Breaches and Security Incidents. BUSINESS ASSOCIATE shall notify UNIVERSITY in writing as soon as possible, but in no event more than two (2) business days, after BUSINESS ASSOCIATE becomes aware of any Breach of Security Incident involving UNIVERSITY’s PHI. BUSINESS ASSOCIATE shall be deemed to be aware of any Breach or Security Incident as of the first day on which such Breach or Security Incident is known or reasonably should have been known to its officers, employees, agents or subcontractors. BUSINESS ASSOCIATE shall identify as soon as practicable each individual whose unsecured PHI has been, or is reasonably believed by BUSINESS ASSOCIATE to have been, accessed, acquired, or disclosed during such Breach or Security Incident. BUSINESS ASSOCIATE shall cooperate in good faith with UNIVERSITY in the investigation of any Breach or Security Incident.

3.8 Prompt Corrective Actions. In addition to the notification requirements in section 3.7 above, and with prior notice to the UNIVERSITY, BUSINESS ASSOCIATE shall take (i) prompt corrective action to remedy any Breach or Security Incident, (ii) mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by BUSINESS ASSOCIATE, and (iii) take any other action required by applicable federal and state laws and regulations pertaining to such Breach or Security Incident.

3.8.1 Notification of Corrective Action and Provision of Policies. BUSINESS ASSOCIATE will provide written notice to UNIVERSITY as soon as possible but no later than twenty (20) calendar days after discovery of the Breach or Security Incident of (i) the actions taken by BUSINESS ASSOCIATE to mitigate any harmful effect of such Breach or Security Incident and (ii) the corrective action BUSINESS ASSOCIATE has taken or shall take to prevent future similar Breaches or Security Incidents. Upon UNIVERSITY’s request, BUSINESS ASSOCIATE will also provide to UNIVERSITY a copy of BUSINESS ASSOCIATE’s policies and procedures that pertain to the Breach or Security Incident involving UNIVERSITY’s PHI, including procedures for curing any material breach of this BA AGREEMENT.

3.8.2 Lost or Indecipherable Transmissions. BUSINESS ASSOCIATE agrees to make reasonable efforts to trace lost or translate indecipherable transmissions. BUSINESS ASSOCIATE shall bear all costs associated with the recreation of incomplete, lost or indecipherable transmissions if such loss is the result of an act or omission of BUSINESS ASSOCIATE.

3.9 RIGHTS and RESPONSIBILITIES of UNIVERSITY.

3.9.1 Right of UNIVERSITY to Accounting or Audit. Within fifteen (15) calendar days of UNIVERSITY’s request, BUSINESS ASSOCIATE shall provide, at BUSINESS ASSOCIATE’s expense, an audit or written accounting of the uses and disclosures of UNIVERSITY’s PHI made by BUSINESS ASSOCIATE and its Agents, if: (i) UNIVERSITY receives credible information that there has been a Breach or Security Incident involving UNIVERSITY’s PHI, or (ii) if UNIVERSITY determines that the written notice provided in section 3.8.1 does not provide sufficient assurances that the Breach or Security Incident involving UNIVERSITY’s PHI has been remedied.

3.9.2 UNIVERSITY’s Right to Terminate. If BUSINESS ASSOCIATE fails to
provide the accounting or audit in a timely manner, or if UNIVERSITY is not satisfied that the corrective action is sufficient to reasonably prevent similar Breaches or Security Incidents in the future, UNIVERSITY may terminate its applicable agreements with BA in accordance with section 5, below.

3.9.3 Costs Related to Inappropriate Use, Access or Disclosure of PHI. If BUSINESS ASSOCIATE fails to adhere to any of the privacy, confidentiality, and/or data security provisions set forth in this BA AGREEMENT or any other agreement it has with UNIVERSITY or if there is a Security Incident or Breach of PHI in BUSINESS ASSOCIATE’s possession and, as a result, PHI or any other confidential information is unlawfully accessed, used or disclosed, BUSINESS ASSOCIATE agrees to pay and reimburse UNIVERSITY for any and all costs, direct or indirect, incurred by UNIVERSITY associated with any Security Incident or Breach notification obligations. BUSINESS ASSOCIATE also agrees to pay for any and all fines and/or administrative penalties imposed for such unauthorized access, use or disclosure of confidential information or for delayed reporting if it fails to notify the UNIVERSITY of the Breach or Security Incident as required by this BA AGREEMENT.

3.9.4 Regulatory Compliance. BUSINESS ASSOCIATE shall make its internal practices, books and records relating to the use, disclosure or security of PHI received from UNIVERSITY (or created or received by BUSINESS ASSOCIATE on behalf of UNIVERSITY) available to any state or federal agency, including the U.S. Department of Health and Human Services, for purposes of determining UNIVERSITY’s and/or BUSINESS ASSOCIATE’s compliance with federal/state privacy and security laws and regulations.

3.9.5 Inspection of Records. Within thirty (30) calendar days after UNIVERSITY’s written request, BUSINESS ASSOCIATE shall make available to UNIVERSITY and its authorized agents, during normal business hours, all facilities, systems, procedures, records, books, agreements, policies and procedures relating to the use and/or disclosure of UNIVERSITY’s PHI for purposes of enabling UNIVERSITY to determine BUSINESS ASSOCIATE’s compliance with federal/state privacy and security laws and regulations.

3.10 Rights of Individuals.

3.10.1 Individual’s Right to Request Restrictions of PHI. BUSINESS ASSOCIATE shall notify UNIVERSITY in writing within five (5) business days after receipt of any request by individuals or their representatives to restrict the use and disclosure of the PHI BUSINESS ASSOCIATE maintains for or on behalf of UNIVERSITY. Upon written notice from UNIVERSITY that it agrees to comply with the requested restrictions, BUSINESS ASSOCIATE agrees to comply with any instructions to modify, delete or otherwise restrict the use and disclosure of PHI it maintains for or on behalf of UNIVERSITY.

3.10.2 Individual’s Request for Amendment of PHI. BUSINESS ASSOCIATE shall inform UNIVERSITY within five (5) business days after receipt of any request by or on behalf of the subject of the PHI to amend the PHI that BUSINESS ASSOCIATE maintains for or on behalf of UNIVERSITY. BUSINESS ASSOCIATE shall, within twenty (20) calendar days after receipt of a written request, make the subject’s PHI available to UNIVERSITY as may be required to fulfill UNIVERSITY’s obligations to amend PHI pursuant to HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR § 164.526. BUSINESS ASSOCIATE shall, as directed by UNIVERSITY, incorporate any amendments to UNIVERSITY’s PHI into copies of such PHI
maintained by BUSINESS ASSOCIATE.

3.10.3 Individual’s Request for an Accounting of Disclosures of PHI. BUSINESS ASSOCIATE shall document all disclosures of PHI and, within twenty (20) calendar days after receipt of a written request, make available to UNIVERSITY, and, if authorized in writing by UNIVERSITY, to the subject of the PHI, such information maintained by BUSINESS ASSOCIATE or its agents as may be required to fulfill UNIVERSITY’s obligations to provide an accounting for disclosures of UNIVERSITY’s PHI pursuant to HIPAA, the HIPAA Regulations, including, but not limited to, 45 CFR § 164.528, and the HITECH Act, including, but not limited to Section 13405(c).

3.10.4 Electronic Health Records. If BUSINESS ASSOCIATE, on behalf of UNIVERSITY, uses or maintains Electronic Health Records with respect to PHI, UNIVERSITY may provide an individual, upon the individual’s request, with the name and contact information of BUSINESS ASSOCIATE so that the individual may make a direct request to BUSINESS ASSOCIATE for an accounting of disclosures made by BUSINESS ASSOCIATE during the three (3) years prior to the date on which the accounting is requested or as otherwise provided under the HITECH Act Section 13405(c)(4)(A) or Section 13405(c)(4)(B).

3.10.5 Access to PHI by the Individual. If UNIVERSITY determines that a an individual’s PHI is held solely by BUSINESS ASSOCIATE or if BUSINESS ASSOCIATE is acting on behalf of UNIVERSITY to provide access to or a copy of an individual’s PHI, BUSINESS ASSOCIATE shall, within five (5) calendar days after receipt of a written request, make available to UNIVERSITY, and, if authorized in writing by UNIVERSITY, to the subject of the PHI, such information as may be required to fulfill UNIVERSITY’s obligations to provide access to or provide a copy of the PHI pursuant to HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR § 164.524.

3.10.6 Access to Certain Information in Electronic Format. If BUSINESS ASSOCIATE uses or maintains Electronic Health Records with respect to PHI on behalf of UNIVERSITY, BUSINESS ASSOCIATE shall, upon request of UNIVERSITY, provide UNIVERSITY with the requested Electronic Health Record in an electronic format.

3.11 Compliance with Law. In connection with all matters related to this BA AGREEMENT, BUSINESS ASSOCIATE shall comply with all applicable federal and state laws and regulations, including, but not limited to, HIPAA, the HIPAA Regulations, 45 CFR §§ Parts 160, 162 and 164, and the HITECH Act, Subtitle D, part 1, California Civil Code §1798.29 and California Health and Safety Code §1280.15, as they may be amended from time to time.

4. BUSINESS ASSOCIATE’S AGENTS. Other than as expressly authorized herein, BUSINESS ASSOCIATE will provide UNIVERSITY’s PHI only to persons or entities, including subcontractors, that have an agency relationship to BUSINESS ASSOCIATE and that have been approved in advance by UNIVERSITY ("Agents"). BUSINESS ASSOCIATE will provide PHI to Agents solely for the purposes of carrying out the Agreement.

4.1 BUSINESS ASSOCIATE shall require such Agents to agree to the same restrictions and conditions that are imposed on BUSINESS ASSOCIATE by this BA AGREEMENT, and to provide written assurance of such agreement, including, but not limited to, sections 3.5 ("Security Standards"), 3.6 ("Security Documentation") and 3.7 ("Notification of Breaches and
Security Incidents).

5. TERMINATION AND OTHER REMEDIES.

5.1 Material Breach. A breach by either party of any material provision of this BA AGREEMENT shall constitute a material breach of the agreement(s) between UNIVERSITY and BUSINESS ASSOCIATE. Either party, upon written notice to the other party describing the breach, may take any of the following actions:

5.1.1 Terminate all applicable agreements, including this BA AGREEMENT, immediately if the other party has breached a material term of this BA AGREEMENT.

5.1.2 Terminate the applicable agreement(s), including this BA AGREEMENT, unless the other party, within five (5) business days, provides a plan to cure the breach and, within fifteen (15) business days, cures the breach;

5.1.3 In the case of a material breach of the BA AGREEMENT, if termination is not feasible, upon the non-breaching party’s request, the breaching party shall:

   (a) at its expense, provide a third-party review of the outcome of any plan implemented under section 5.1.2. to cure the breach;

   (b) at its expense, submit to a plan of monitoring and reporting to demonstrate compliance with the BA AGREEMENT.

5.2 Effect of Termination - Return or Destruction of PHI held by BUSINESS ASSOCIATE or BUSINESS ASSOCIATE’s Agents. Upon termination, expiration or other conclusion of the BA AGREEMENT for any reason, BUSINESS ASSOCIATE shall return or, at the option of UNIVERSITY, provide for the Destruction of all PHI received from UNIVERSITY, or created and received by BUSINESS ASSOCIATE on behalf of UNIVERSITY in connection with the BA AGREEMENT, that BUSINESS ASSOCIATE or its Agents still maintains in any form, and shall retain no copies of such PHI. Within thirty (30) calendar days after the termination of this BA AGREEMENT, BUSINESS ASSOCIATE shall both complete such return or Destruction and certify in writing to UNIVERSITY that such return or Destruction has been completed.

5.3 Return or Destruction Not Feasible. If BUSINESS ASSOCIATE represents to UNIVERSITY that return or Destruction of UNIVERSITY’s PHI is not feasible, BUSINESS ASSOCIATE must provide UNIVERSITY with a written statement of the reason that return or Destruction by BUSINESS ASSOCIATE or its Agents is not feasible. If UNIVERSITY determines that return or Destruction is not feasible, this BA AGREEMENT shall remain in full force and effect and shall be applicable to any and all of UNIVERSITY’s PHI held by BUSINESS ASSOCIATE or its Agents.

5.4 Other Remedies. Notwithstanding the foregoing rights to terminate the Agreement, UNIVERSITY shall have such other remedies as are reasonably available at law or equity, including injunctive relief.

5.5 Civil and Criminal Penalties. BUSINESS ASSOCIATE understands and agrees that it is subject to civil or criminal penalties applicable to BUSINESS ASSOCIATE for unauthorized
use, access or disclosure of PHI in accordance with the HIPAA Regulations and the HITECH Act.

6. **CHANGES TO THIS BA AGREEMENT.**

   6.1 Compliance with Law. The parties acknowledge that state and federal laws and regulations relating to electronic data security and privacy are rapidly evolving and that additional obligations and responsibilities may be imposed on BUSINESS ASSOCIATE to ensure compliance with the new laws and regulations. The parties specifically agree to comply with all applicable laws and regulations and take such action as may be necessary to implement the standards and requirements of HIPAA, the HIPAA Regulations, the HITECH Act, and other applicable state and federal laws and regulations relating to the security or confidentiality of PHI, without need to amend or modify this BA AGREEMENT.

7. **INSURANCE AND INDEMNIFICATION.**

   7.1 Insurance. In addition to any general and/or professional liability insurance coverage required of BUSINESS ASSOCIATE under the 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 and expenses arising from a breach of the security, privacy, or confidentiality obligations of BUSINESS ASSOCIATE, its officers, employees, agents and subcontractors, under this BA AGREEMENT. Such insurance coverage shall be maintained for the term of the Agreement, and a copy of such policy or a certificate evidencing the policy shall be provided to UNIVERSITY at UNIVERSITY’s request.

   7.2 Indemnification by BUSINESS ASSOCIATE. BUSINESS ASSOCIATE agrees to defend at UNIVERSITY’s election, indemnify, and hold harmless UNIVERSITY, its officers, agents or employees from and against any and all claims, liabilities, demands, damages, losses, costs and expenses (including costs and reasonable attorneys’ fees), or claims for injury or damages that are caused by or result from the acts or omissions of BUSINESS ASSOCIATE, its officers, employees, agents and subcontractors with respect to the use and disclosure of UNIVERSITY’s PHI.

   7.3 Indemnification by UNIVERSITY. UNIVERSITY agrees to defend at BUSINESS ASSOCIATE’s election, indemnify, and hold harmless BUSINESS ASSOCIATE, its officers, agents and employees from and against any and all claims, liabilities, demands, damages, losses, costs and expenses (including costs and reasonable attorneys’ fees), or claims for injury or damages that are caused by or result from the acts or omissions of UNIVERSITY, its officers, agents or employees with respect to the use and disclosure of UNIVERSITY’s PHI.

8. **MISCELLANEOUS PROVISIONS.**

   8.1 Assistance in Litigation or Administrative Proceedings. BUSINESS ASSOCIATE shall make itself, and any employees or agents assisting BUSINESS ASSOCIATE in the performance of its obligations under this BA AGREEMENT, available to UNIVERSITY at no cost to UNIVERSITY to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings against UNIVERSITY, its directors, officers, agents or employees based upon claimed violation of HIPAA, the HIPAA Regulations or other laws relating to security and privacy.
8.2 Independent Contractor. BUSINESS ASSOCIATE is an independent contractor and nothing in this BA AGREEMENT is intended to create or imply an agency or employment relationship between UNIVERSITY and BUSINESS ASSOCIATE.

8.3 No Third-Party Beneficiaries. Nothing express or implied in this BA AGREEMENT is intended to confer, nor shall anything herein confer, any rights, remedies, obligations or liabilities whatsoever upon any person or entity other than UNIVERSITY, BUSINESS ASSOCIATE and its respective agents, successors or assigns.

8.4 Number. Where the context admits, words in the plural include the singular, and the singular includes the plural.

8.5 Survival. The obligations of BUSINESS ASSOCIATE under Sections 3.3, 3.4, 3.5 3.6, 3.7, 3.8, 3.9, 3.10, 5.2, 5.3, 5.5, 7.2, 7.3, and 8.1 of this BA AGREEMENT shall survive the termination of any agreement between UNIVERSITY and BUSINESS ASSOCIATE.

8.6 Notices. Any notices to be given to either party shall be made via U.S. Mail or express courier to the address given below and/or via facsimile to the facsimile telephone numbers listed below.

If to BUSINESS ASSOCIATE, to: 

__________________________________________

__________________________________________

Attention: ________________________________

Fax: ________________________________

With a copy (which shall not constitute notice) to:

__________________________________________

__________________________________________

Attention: ________________________________

Fax: ________________________________

If to UNIVERSITY, to: 

__________________________________________

__________________________________________

Attention: ________________________________

Fax: ________________________________

With a copy (which shall not constitute notice) to:

__________________________________________

__________________________________________

Attention: ________________________________

Fax: ________________________________

Each party may change its address and that of its representative for notice by giving notice in the manner provided above.
IN WITNESS WHEREOF, the parties hereto have duly executed this BA AGREEMENT.

The Regents of the University of California on behalf of its University of California Health System

[Name of BUSINESS ASSOCIATE]

Signature

Signature

Printed Name

Printed Name

Title

Title

Date

Date
Appendix B

UC Riverside Decision Tree for Determining BAA Relationship

General Instructions:

1. If the Business Associate requests any changes to the BAA agreement other than allowed in the UC Annotated BAA agreement, refer the agreement to the Privacy Officer for review.
2. If the Business Associate agrees to the terms of the standardized UC Agreement forward one copy of the signed original to the Purchasing Director and return one signed original to the Business Associate.
3. If the agreement is a UC wide agreement the Purchasing Director will upload a copy to the system-wide database.

NOTE: TRACK PROGRESS Through the decision tree by placing a checkmark in circle.

What type of contract is this?

- Type: Maintenance
  - Lease/Service/Lease Renewal
    - i.e. Copiers, scanners, computer equipment, electronic devices, medical equipment etc.
  - Maintenance/Service

- Type: Consulting/contractor (Service Agreement, Patient Safety Org, HIE, system or person needing routine access to PHI)

- Type: Supply/Contract

Does this machine store PHI?

- Yes
  - Does Vendor have access to PHI during maintenance?
    - Yes
      - Does person have more than an "incidental" access to PHI? If yes, describe in space below.
      - Yes
        - BAA Needed, Forward Purchase Regulation, this BAA Analysis, and other related documents to the Purchasing Contracting Officer/Attorney
      - No
        - No BAA Needed
        - Reminder: Vendor on site must comply with UCR Vendor policy and vendor guide including signing individual confidentiality agreement.
        - Is there the possibility of disclosure of PHI?
          - Incidental PHI (seen in the course of doing on the premises but no receiving or accessing PHI as part of BAA function)
          - No PHI

Legend:
- BAA - Business Associate
- BAA Business Associate Agreement
- HIPAA - Health Insurance Portability and Accessibility Act
- PHI - Protected Health Information
- Policies Referenced: HIPAA, Business Associate Agreement

To Be Completed by Person conducting Analysis:

VENDOR NAME: ____________________________

SIGNATURE: ____________________________

DATE: ____________________________

Purchase Order #: ____________________________
Please describe access to PHI by Vendor (continued from previous slide)


For questions, please contact the Purchasing Office or the Privacy Officer.