

UC Riverside, School of Medicine Policies and Procedures

Policy Title: Business Associate Agreement

Policy Number: 950-02-037

Responsible Officer:	Chief Compliance & Privacy Officer
Responsible Office:	Compliance Advisory Services
Origination Date:	06/2013
Date of Revision:	03/07/2024
Scope:	UCR Health

I. Policy Summary

UCR Health periodically engages the services of third parties whose work requires access, use or disclosure of Protected Health Information (“PHI”). These third parties are known as Business Associates. UCR Health may disclose Protected Health Information to a Business Associate if UCR Health obtains satisfactory assurances that the Business Associate will appropriately safeguard that information.

This policy establishes how UCR Health shall obtain satisfactory assurances from Business Associates through the contractual agreements required under the HIPAA privacy and security standards. This policy also describes the required reporting of contract violations and potential Breaches caused by the Business Associate.

II. Definitions

Accounting of Disclosures: A record of certain disclosures of PHI made by a Covered Entity within the prior six years that a Covered Entity must give a patient at their request. Disclosures made for purposes of Treatment, Payment, or Healthcare Operations (TPO), with a patient's Authorization, or as otherwise described under 45 CFR sec.164.528 are excluded from an accounting.

Breach: The acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA privacy regulations which compromises the security or privacy of the PHI.

Business Associate (BA): A person or entity that creates, receives, maintains, transmits, or otherwise discloses protected health information (PHI) as a result of providing services to or for a Covered Entity. Specific functions or activities that could create a Business Associate relationship include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management, or re-pricing, legal, actuarial, consulting, data aggregation, management, administrative, accreditation, software support requiring routine access to PHI, financial and/or accounting services. Business Associates may include Patient Safety Organizations and Health Information Exchanges (HIE's). Covered Entity Workforce Members, members of an Organized Healthcare Arrangement, and healthcare providers involved in a particular individual’s treatment typically are not Business Associates.

Covered Entity (CE): An entity that must comply with HIPAA. Covered Entities specifically refer to healthcare providers that transmit certain health information in electronic form, health plans, and healthcare clearinghouses.

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

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.

For other definitions in this policy, refer to the HIPAA privacy and security implementing regulations at 45 CFR Parts 160, 162, and 164.

III. Policy Text

- A. As a HIPAA Covered Entity, UCR Health may only share Protected Health Information (PHI) with a Business Associate, or allow a Business Associate to create, receive, or use PHI for or on behalf of UCR Health, when an approved and executed written Business Associate Agreement (BAA) is in place. The BAA is executed in the form of a Business Associate Addendum to an University-approved procurement agreement. Each BAA must contain the current UC system-wide approved BAA language and authorized signatures. Any changes to the UC System-wide approved language may only be approved by the UCR School of Medicine Chief Compliance and Privacy Officer, Purchasing Officer, Campus Legal Counsel, or Risk Manager.
- B. It is the responsibility of each UCR School of Medicine department, division, or operating unit arranging for services with third parties where PHI will be shared, to assure that valid BAAs are executed prior to the disclosure of any PHI.
- C. UCR Health is not required to enter into a BAA with other treating health care provider(s) prior to disclosing PHI or other information related to treatment of an individual.
- D. Individual members of UCR Health have an obligation to timely notify their manager or the UCR School of Medicine Chief Compliance and Privacy Officer if they become aware of a potential or actual Business Associate Agreement violation.
- E. Any time UCR Health determines that a Business Associate has violated a material term or obligation of the BAA, the department that is party to the agreement and the UCR School of Medicine Chief Compliance and Privacy Officer shall be notified and shall seek to take reasonable steps to remedy the breach.
- F. If it is not possible to remedy the breach, UCR Health and/or the University will move to terminate the agreement if feasible. To the extent required by law, violations will be reported to the Secretary of the Department of Health & Human Services.

IV. Responsibilities

- A. All Health Sciences Personnel
- B. Procurement
- C. School of Medicine Chief Compliance and Privacy Officer

V. Procedures

- A. Department/Division/Procurement Responsibility

1. UCR Procurement is responsible for determining whether a BAA is necessary for any third-party service arrangements requested by a UCR School of Medicine department. Procurement may consult with the School of Medicine Chief Compliance and Privacy Officer to determine whether a BAA is necessary.
 2. Vendors should be presented with the approved UC system-wide BAA. Any requests for alternative language must be approved by authorized UCR personnel.
 3. Only a UCR Campus Procurement Officer who has delegated responsibility is authorized to sign a BAA on behalf of the University of California.
 4. Procurement may confer with other UC campuses to determine if a System-wide Business Associate Agreement currently is in place with the Business Associate.
 5. Arrangements that are unclear as to status must be referred to the School of Medicine Chief Compliance and Privacy Officer for further determination.
 6. UCR shall undertake reasonable diligence prior to contracting with a Business Associate.
- B. Responsibilities of the Business Associate:** The UC-System BAA sets forth the actions for which the Business Associate will be responsible.
- C. Common Situations that Do Not Require a Business Associate Agreement:** The following situations do not require a BAA:
1. PHI used and disclosed for treatment, payment and health care operations (TPO), including PHI sharing among UCR Health workforce members;
 2. Disclosure for financial transactions, e.g., bank or credit card transactions of a UCR Health patient to pay a bill for health care services;
 3. Disclosures between group health plans and the University of California as a health plan sponsor;
 4. Disclosures to other CEs for purposes of treating a shared patient;
 5. Disclosures to another CE for health care operations of the receiving entity, so long the patient has a relationship with both UCR and the other entity, the PHI requested pertains to that relationship, and the disclosure is for the detection of fraud or abuse.
 6. Disclosures to other contracted individuals and volunteers or trainees if they function as a member of UCR's workforce and receive privacy training.
 7. Disclosures to couriers where the person is a conduit or carrier of PHI.
 8. Disclosures of PHI between UCR and affiliated training institutions as necessary to carry out training and educational programs, as well as to meet the accreditation and licensing requirements of each institution.
- D. Questions and Communications:** Communication regarding confidentiality and privacy policies and monitoring shall be channeled through the UCR School of Medicine Chief Compliance and Privacy Officer (951-827-4672).
- E. Accounting for Disclosures:** Ordinarily disclosures of PHI to a BA used under a BAA need not be included in a HIPAA accounting; however, disclosures of PHI for non-permitted uses must be logged and made available to the patient upon request.
- F. Reporting Violations:** All known or suspected violations of this policy should be reported to the School of Medicine Chief Compliance and Privacy Officer, Human Resources, the UCR Confidential Compliance Message Line (1-800-403-4744), or the UCR Chief Compliance Officer at <https://compliance.ucr.edu/>.
- G. 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.

VI. Forms/Instructions

- A. Appendix A: UC System-Wide Business Associate Agreement (The University of California may update this agreement from time to time. Contact UCR Procurement for the most current version.)

VII. Related Information

- 45 C.F.R. sec 164.502(e), 45 C.F.R. sec 164.504(e), 45 CFR sec. 164.314
- 45 C.F.R. Part 164, Subpart D
- California Civil Code §§1798.82
- <https://policy.ucop.edu/doc/1110160/HIPAA-3>
- UCR SOM Policy 950-02-015 (HIPAA Breach Risk Assessment and Mitigation)
- UCR SOM Policy 950-02-225 (Privacy and Security Breach Response and Incident Notification)

Approvals:

COMPLIANCE COMMITTEE (09/03/2024)

Signed by: *Paul Hackman* 9/20/2024 | 10:59 PM PDT

 BC5CF44DC0494EA...
 PAUL HACKMAN, J.D., L.L.M. DATE
 CHIEF COMPLIANCE AND PRIVACY OFFICER,
 SCHOOL OF MEDICINE

Signed by: *Deborah Deas* 9/21/2024 | 4:45 PM PDT

 870C12B416E87CB...
 DEBORAH DEAS, M.D., M.P.H. DATE
 VICE CHANCELLOR, HEALTH SCIENCES
 DEAN, SCHOOL OF MEDICINE



UNIVERSITY OF CALIFORNIA

Appendix – Business Associate Agreement

This Appendix - Business Associate Agreement ("Appendix BAA") 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 ("UC"), on behalf of its University of California Health System and _____, Business Associate ("BA").

RECITALS

- A. UC is a "Covered Entity" as defined under 45 C.F.R. § 160.103
- B. UC and BA are entering into or have entered into, and may in the future enter into, one or more agreements (each an "Underlying Agreement") under which BA performs functions or activities for or on behalf of, or provides services to UC ("Services") that involve receiving, creating, maintaining and/or transmitting Protected Health Information ("PHI") of UC as a "Business Associate" of UC as defined under 45 C.F.R. § 160.103. This Appendix BAA shall only be operative in the event and to the extent this Appendix BAA is incorporated into an Underlying Agreement between UC and BA.
- C. UC and BA desire to protect the privacy and provide for the security of PHI used by or disclosed to BA 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 C.F.R. Parts 160, 162 and 164) (the "HIPAA Regulations"), the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act"), California Civil Code § 56 et seq., §§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), the HITECH Act, including Subtitle D, part 1, as they may be amended from time to time, and similar requirements under California law.
- D. UC has designated all of its HIPAA health care components as a single component of its hybrid entity and therefore this BA Agreement is binding on all other UC health care components (collectively, the Single Health Care Component or the SHCC). This BA Agreement is effective on the date of the Underlying Agreement under which BA provides Services to UC ("Effective Date").

1. DEFINITIONS

Except for PHI, all capitalized terms in this Appendix BAA shall have the same meaning as those terms in the HIPAA Regulations.

PHI shall have the same meaning as "protected health information" in the HIPAA Regulations that is created, received, maintained, or transmitted by Business Associate or any Subcontractor on behalf of UC and shall also include "medical information" as defined at Cal. Civ. Code § 56.05.

2. OBLIGATIONS OF BA

BA agrees to:

- A. Comply with the requirements of the Privacy Rule that apply to UC in carrying out such obligations, to the extent BA carries out any obligations of UC under the Privacy Rule. BA also agrees to comply with the requirements of California state privacy laws and regulations that apply to UC in carrying out such obligations, to the extent BA carries out any obligations of UC under California Civil Code § 1798 et seq., California Civil Code § 56 et seq., and California Health & Safety Code §§ 1280.15 and 1280.18, as applicable, unless otherwise mutually agreed to by BA and UC.
- B. Not Use or Disclose PHI other than as permitted or required by the Underlying Agreement or as required by law.
- C. Use appropriate safeguards, and comply, where applicable, with 45 C.F.R. § 164 Subpart C with respect to ePHI, to prevent the Use or Disclosure of PHI other than as provided for by the Underlying Agreement(s) and the Appendix BAA.
- D. Notify UC, orally and in writing, as soon as possible, but in no event more than five (5) calendar days, after BA becomes aware of any Use or Disclosure of the PHI not permitted or required by the Appendix BAA or Underlying Agreement(s), including Breaches of unsecured PHI as required by 45 C.F.R. § 164.410 and potential compromises of UC PHI, including potential inappropriate access, acquisition, use or disclosure of UC PHI (each, collectively an “Incident”). BA shall be deemed to be aware of any such Incident, as of the first day on which it becomes aware of it, or by exercising reasonable diligence, should have been known to its officers, employees, agents or sub-suppliers. The notification to UC shall include, to the extent possible, each individual whose unsecured PHI has been, or is reasonably believed by BA to have been, accessed, acquired, used or disclosed during such Incident. BA shall further provide UC with any other available information that UC is required to include in a notification to affected individuals at the time of the notification to UC, or promptly thereafter as information becomes available. BA shall take prompt corrective action to remedy any such Incident, and, as soon as possible, shall provide to UC in writing: (i) the actions initiated by the BA to mitigate, to the extent practicable, any harmful effect of such Incident; and (ii) the corrective action BA has initiated or plans to initiate to prevent future similar Incidents.
- E. Ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same restrictions, conditions, and requirements that apply to the BA with respect to such PHI.
- F. If BA maintains PHI in a Designated Record Set, BA shall make the PHI in the Designated Record Set available to UC, or if directed by UC to the Individual or the Individual’s designee, as necessary to satisfy UC’s obligations under 45 C.F.R. § 164.524.
- G. If BA maintains PHI in a Designated Record Set, BA shall make any amendments directed or agreed to by UC pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy UC’s obligations under 45 C.F.R. § 164.526.

- H. Maintain and make available the information required to provide an accounting of disclosures to UC, or if directed by UC to the Individual, as necessary to satisfy UC’s obligations under 45 C.F.R. § 164.528.
- I. Make its internal practices, books, and records, relating to the Use and Disclosure of PHI available to UC, and to the Secretary for purposes of determining UC’s compliance with HIPAA, HITECH and their implementing regulations.

3. PERMITTED USES AND DISCLOSURES BY BA

BA may only Use or Disclose the Minimum Necessary PHI to perform the services set forth in the Underlying Agreement.

4. TERM AND TERMINATION

- A. Termination for Cause. UC may terminate this Appendix BAA and any Underlying Agreement(s), if UC determines BA has violated a material term of the Appendix BAA.
- B. Upon termination of this Appendix BAA for any reason, with respect to PHI received from UC, or created, maintained, or received by BA on behalf of UC, BA shall return to UC, or if agreed to by UC, destroy, all such PHI that BA still maintains in any form, and retain no copies of such PHI.


To the extent return or destruction of UC PHI is not feasible, BA shall (1) retain only that PHI which is necessary for BA to continue its proper management and administration or to carry out its legal responsibilities; and (2) continue to use appropriate safeguards for such UC PHI and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI to prevent Use or Disclosure of the PHI, other than as provided for in this Section, for as long as BA retains the PHI.

- C. Survival. The obligations of BA under this Section 4.B shall survive the termination of this Appendix BAA and any Underlying Agreement(s).

The Appendix BAA is signed below by the parties’ duly authorized representatives.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

BUSINESS ASSOCIATE



 (Signature)

Paul Williams, Chief Procurement Officer
(Printed Name, Title)

August 10, 2021
(Date)

(Supplier Name)

(Signature)

(Printed Name, Title)

(Date)