THE REGENTS OF THE UNIVERSITY OF CALIFORNIA
OFFICE OF THE GENERAL COUNSEL

BERKELEY * DAVIS * IRVINE * LOS ANGELES * MERCED * RIVERSIDE * SAN DIEGO * SAN FRANCISCO
SANTA BARBARA * SANTA CRUZ

1111 Franklin Street, 8th Floor * Oakland, California 94607

Charles F. Robinson
VICE PRESIDENT AND GENERAL COUNSEL

Writer's direct line: (510) 987-9357
E-mail: Susan.Stayn@ucop.edu

Re: Retention for Health Affairs, Privacy & Data Protection Law Matters

Dear :

As you know, the General Counsel has established a Health Affairs, Privacy & Data Protection ("HAPDP") Section within UC Legal, which is comprised of the Office of the General Counsel in Oakland, California ("OGC") and Offices of Legal Affairs at individual University locations ("OLAs"). The HAPDP Section is divided into a Health Law Group and a Privacy & Data Protection Group. The health law practice group primarily supports UC's clinical and related research and teaching operations (collectively known as "UC Health") located throughout the UC System – *see* http://health.universityofcalifornia.edu/. UC Health includes five full-service academic health systems at the Davis, Irvine, Los Angeles, San Diego, and San Francisco campuses comprised of hospitals, medical schools, faculty practice plans, and other facilities and providers, an additional medical school at the Riverside campus, and other health professions schools throughout the State of California. The Health Law Group also supports the University's community hospitals, student health and counseling centers. The Privacy & Data Protection Group handles privacy, cybersecurity, and other technology matters across the UC system. We also support advocacy and litigation efforts on behalf of the University within these practice areas.

The HAPDP Section works continuously to secure high-quality, cost-effective legal services to complement the University's expert in-house team; and to streamline our processes for choosing and retaining counsel and for payment of legal services in connection with individual transactions, regulatory matters, government investigations, certain litigation, and other matters. 's team has demonstrated requisite expertise and experience in one or more applicable subfields. Specifically, ("Firm") is a member of the HAPDP Preferred Provider Panel, effective _____, 2025, as follows: .

This letter will serve as the master retention for your firm's legal services during the course of your engagement or engagements on UC Health, Privacy and Data Protection matters. An individual HAPDP matter may be initiated only by completion and execution of the form

appended to this letter as Attachment 1-Health, Privacy & Data Protection Law Matter Retention Schedule (a "Retention Schedule").

Nothing contained in these guidelines is intended, nor shall they be interpreted, to restrict any attorney's independent exercise of professional judgment in rendering legal services to the University, or otherwise to interfere with any ethical obligation governing the conduct of an attorney.

Compliance with Outside Counsel Guidelines and University Contacts

Firm's retention on any individual matter is made on behalf of The Regents of the University of California by an authorized UC Legal attorney, typically a Deputy General Counsel. That or another attorney – a "UC Legal Monitor" resident in the Oakland Office ("Oakland Monitor"), and/or at a campus or medical center ("Local Monitor"), is responsible for day-to-day work and oversight of the matter, subject to supervision by the Chief Campus Counsel and/or Deputy General Counsel ("Supervising Attorney(s)"). Firm may communicate directly with internal clients to facilitate a representation, but UC Legal maintains exclusive authority to direct Firm in the handling of the matter and must be kept apprised of all significant developments and advice given.

Firm's services will be performed consistent with this letter, the University's outside billing guidelines, as amended from time to time, included here in their current form as Attachment 2-University of California Outside Counsel Billing Guidelines; and, if and to the extent applicable to a given matter, the Business Associate Agreement included here as Attachment 3-Business Associate Agreement, as well as Attachment 4-Panel Requirements and Terms and Conditions of the UC Legal Health Affairs, Privacy & Data Protection 2025 - 27 Preferred Provider Program Request for Proposals as well as other guidelines and directives issued by UC Legal or HAPDP from time to time (collectively the "Guidelines"), and Attachment 5—Appendix DS.

Participating Attorneys, Rates, and Budgets

As the Relationship Partner(s) for the HAPDP, you will be primarily responsible for the overall relationship between Firm and UC with respect to matters initiated under this master retention letter, and to assure Firm's compliance with the Guidelines in connection with any representation. You are also expected to familiarize yourself – at your cost – with the governance structure, principal policies, and core values of the University and to assure that Firm's legal services are delivered consistent with these and with the business or operational objectives set for a given matter. The UC Legal Monitors will be most happy to facilitate your efforts in this regard, as will I.

Your firm's work on a matter may be assigned to you or to other attorneys, consultants, and paraprofessionals in your firm listed on Attachment 6-Approved Timekeepers Schedule and on the matter-specific Retention Schedule. ***Absent prior written approval by me or by a UC Legal Monitor, work performed by timekeepers not listed on the Approved Timekeepers Schedule and the matter-specific Retention Schedule may not be reimbursed.***

Communications with University Counsel

We view open and continuous communication between outside and in-house counsel as essential to ensuring efficient handling of a matter and the best possible results for the University. Accordingly, the UC Legal Monitor must be fully apprised and kept current on all developments and participate in all decisions concerning legal tactics and strategy. Make sure to provide the UC Legal Monitor or designee with copies of all legal opinions and advice, as well as major correspondence, preferably in electronic form. Drafts of significant documents (e.g., agency submissions, definitive agreements, advice memoranda and formal opinions, etc.) should be provided in time for thorough review and discussion. Copies of all significant documents (e.g., filed briefs, formal opinions, definitive agreements) must be provided to the UC Monitor and to me. Failure to provide this work product to a UC Monitor may result in non-payment.

Use of Name; Media Communications

Firm acknowledges that use of the University's name is governed by Cal. Ed. Code §§ 92000. Firm will not initiate or respond to media communications related to University matters for any purpose without the University's prior authorization. If media exposure or contact is anticipated or occurs, Firm will immediately notify the UC Legal Monitor(s) and Supervising Attorney(s) so that appropriate stakeholders may be notified and preparations may be made.

Philosophy on Conflicts and Conflict Waivers

To request a conflict waiver, simply contact my Executive Assistant, Kerry Meech (Kerry.Meech@ucop.edu or 510-987-9043) and provide the relevant information. We aim to respond expeditiously. Please note that the University does *not* approve advance or blanket waivers of future conflicts, whether client-specific or otherwise, except under extraordinary circumstances and subject to specially designed protections developed to protect the University's interests. Our view is that, as a general matter, it is impossible for a firm to adequately disclose the relevant circumstances and actual and reasonably foreseeable adverse consequences of conflicts that have not yet materialized. *See, e.g., Shepard, Mullin, Richter & Hampton, LLP v. J-M Manufacturing Company, Inc.* (Cal 2018)*; Concat LP v. Unilever, PLC*, 350 F. Supp. 2d 796 (N.D. Cal. 2004). Although no advance waivers are approved pursuant to these Guidelines, we do make every effort to promptly respond to individual waiver requests and we routinely waive conflicts, particularly with respect to transactional work.

Political Reform Act

University employees are subject to certain transparency requirements and related restrictions imposed by the California Political Reform Act ("CPRA"). Among other things, CPRA requires annual disclosures by certain public officials, including all UC Legal attorneys, and disqualifies any officials who have defined financial interests from making, participating in, or otherwise influencing certain governmental decisions. UC Legal attorneys may attend firm-sponsored functions and events, but may be required to disclose any resulting gifts on an annual statement that is subject to public disclosure, and depending on the total value of gifts or other

income received in a given year by an attorney and her immediate family from Firm, may be disqualified from engaging Firm on a matter or even making a recommendation regarding an engagement during the subsequent twelve-month period.

Consultants; Firm Work on "Non-Legal" Projects

We recognize that many law firms have created internal consulting practices or have affiliated formally or informally with external consulting firms and that they market this work to health system and higher education executives nationally and locally. Others are occasionally retained by a University Locally Designated Official ("LDO") to perform a whistleblower or retaliation investigation pursuant to the University's whistleblower and whistleblower protection policies. Nothing in this master retention prohibits Firm from performing such work for University clients; provided, however, that: (1) Firm explicitly and in writing notifies the client(s) that its work for them is non-legal (even if performed by lawyers), and is not protected as attorney-client communications or by the attorney work product doctrine and, accordingly, resulting work product may be subject to discovery or public records requests to the same extent it would have been had the work been performed by an external consulting company; and (2) Firm acknowledges, by signing this master retention letter, that only the General Counsel or a Supervising Attorney is authorized to waive any conflicts of interest that Firm may have or later develop with the University. Regardless, we trust that when Firm attaches its name to the work of such consultants, it will assure that such work is high quality and always consistent with applicable law.

Notification of Noncompliance or Misconduct

The University has adopted a Statement of Ethical Values and Standards of Ethical Conduct committing us to integrity, excellence, accountability, and respect in all of our work and dealings. Firm shall immediately report to the Local Monitor (or, if none is identified on a Retention Schedule or in case of a conflict of interest, the Oakland Monitor) any other improper governmental activities ("IGAs"), as defined in the University's Whistleblower Policy, of which Firm becomes aware, regardless of whether such noncompliance or misconduct is the subject of Firm's retention. In the event of professional misconduct involving the UC Monitor, Firm shall report it to the Supervising Attorney. In the event of professional misconduct involving the Supervising Attorney, Firm shall report it to the General Counsel. Firm may also report any IGAs directly to the University's Whistleblower Hotline.

Professionalism; Licensure; Insurance

Commitment to Dignity and Respect. Be nice. We place a high value on treatment of our clients, our leaders, our regulators, our partners, and all of the members of our legal team with compassion, dignity and respect – and expect the same of outside counsel. Incivility, in all of its forms, is demotivating, creates dysfunction, weakens performance, stifles creativity, and substantially increases the risks of errors in judgment and action – for victims of incivility and even for witnesses. Accordingly, rude, disrespectful, and other uncivil behaviors simply will not be tolerated and could result in exclusion of an individual or a Firm from the HAPDP Panel. If a

Firm partner or employee is the victim of such behavior in connection with a University engagement, we want to know that and are committed to taking action to respond appropriately.

Licensure. Firm certifies that all attorneys working on University matters are duly licensed to practice law and are not, and have not previously been, the subject of disciplinary proceedings in any state. Firm shall notify UC Legal promptly of any change in the licensure or certification of any approved timekeeper with any state bar, licensing, or other oversight agency.

Insurance. Firm shall maintain at all times insurance coverage or a self-insurance program appropriate to the nature and scope of its activities including, at a minimum, Errors and Omissions coverage with limits of at least $1 million per claim and $3 million aggregate per attorney. Any deviation from this mandate requires advance written approval from the Supervising Attorney in consultation with the Chief Risk Officer or her designee. Firm shall provide the University with proof of such insurance upon the University's request.

Budgets, Billing Procedures and Reimbursement

Any work performed on an hourly basis requires a budget or retainer. A fee arrangement, budget, or retainer is required for each matter in which Firm has been retained. Although budgets are intended to be estimates of the scope, cost and duration of a given matter, the University will rely on the information provided in planning and funding each matter. We do appreciate that a budget may need to be revised due to circumstances beyond a firm's control, for example unexpectedly difficult opposing counsel or significant changes in the expected scope of a transaction or investigation. It is critical to communicate proactively regarding any anticipated budget overruns. ***The University will not reimburse any fees or costs prior to receipt and approval of a budget nor, thereafter, incurred in excess of the approved budget, except to the extent approved in advance by the UC Legal Monitor and, depending on the scope of the matter, the Deputy General Counsel.***

We expect any attorney, paraprofessional or consultant assuming responsibility for a matter – or for any component of a matter – to have relevant subject matter expertise, training and experience consistent with his or her specialty and rank (e.g., partner, counsel, associate, paralegal, consultant) at Firm; and for Firm as a whole to efficiently and effectively pursue the matter to its conclusion. Basic research on non-novel questions of law should be unnecessary in most cases. The University will not reimburse the costs of researching or preparing legal memoranda, opinions, or similar documents that were not requested or otherwise approved in advance by the UC Legal Monitor, nor those that Firm fails to distribute to the UC Legal Monitor and/or Supervising Attorney (internal memos developed for a firm's benefit are never billable to the University). ***Billing entries for an attorney who allocates significant time to a matter but does not display to the UC Monitor a mastery of the facts and understanding of the applicable law will require justification and may be rejected.***

Fees and other expenses must be charged consistent with the rates specified in the Approved Timekeepers Schedule, approved budgets, and the Guidelines. Invoices must exclude non-reimbursable charges and must be submitted electronically as provided below. ***Failure to***

comply with these requirements may result in delay of payment or non-payment and other corrective action.

Final invoices must be submitted within 30 days from receipt of settlement or other termination of a matter. If the final bill cannot be submitted within 30 days, Firm must advise the UC Legal Monitor as soon as may be practical. It is Firm's responsibility to obtain all outstanding invoices from outside vendors, including consultants and experts, before submitting the final bill. Absent exigent circumstances, bills submitted after the final bill will not be paid.

Any questions concerning billing procedures should be directed to legalbilling@ucop.edu. Requests for invoice payment status should be directed to the applicable UC Legal Monitor with a copy to Kerry Meech (Kerry.Meech@ucop.edu).

Information Security

Firm acknowledges that, in the course of its work, it will receive and produce client confidences. Firm may also receive information protected by federal or state laws or University policies, including without limitation, the Information Practices Act, Cal. Civ. Code 1798 *et seq.* Collectively, these laws and standards require, at a minimum, the adoption of physical, technical, and administrative safeguards sufficient to protect confidential information against unauthorized use, access or disclosure. Firm shall protect all information received, maintained, created, or otherwise collected in the course of its representation of the University consistent with the requirements of the California Rules of Professional Conduct and other applicable law. Firm acknowledges that the California Attorney General has issued guidance on basic measures companies should adopt to secure their records. *See, e.g.,* Cybersecurity in the Golden State (2014) and California Data Breach Report (2016).

* * * * *

We very much appreciate your willingness to represent the University on health law, privacy and data protection matters and look forward to a long and productive working relationship.

Sincerely,

Susan Stayn, Esq.
Deputy General Counsel,
Health Affairs, Privacy & Data Protection Law

SS/km
Agreed and Accepted:

_____

By:

ATTACHMENT 1

Health, Privacy & Data Protection Law Matter Retention Schedule

The firm referenced below ("Firm") is retained to provide legal services to The Regents of the University of California ("UC") and specifically to provide services in connection with the matter described below ("Matter"), subject to the previously executed retention letter and the then-current Guidelines, available online at https://www.ucop.edu/uc-legal/hatl-rfp.html

Campus/Medical Center: **<Choose One>**

Firm Name: _____ Partner in Charge: _____

Matter Name: _____ Matter Number: _____

Matter Type: **<Choose One>** Matter Category (iVos): **<Choose One>**

eBilling Submission System: **<Choose One>**

Matter Description:

Oakland Monitor: _____
Bill Approval? Yes ☐ No ☐ | Budget Approval? Yes ☐ No ☐ | Lead Counsel? Yes ☐ No ☐ N/A ☐

Local Monitor: _____
Bill Approval? Yes ☐ No ☐ | Budget Approval? Yes ☐ No ☐ | Lead Counsel? Yes ☐ No ☐ N/A ☐

Other Key Attorneys (Information/Updates Only): _____

FAU #: _____ FAU Contact Name/Number: _____

Client/Sponsor Name: _____

Assigned Timekeepers:

Note: UC will not reimburse fees incurred in connection with the Matter by or on behalf of any attorney, consultant, paraprofessional, or other timekeeper who is not listed on the Approved Timekeepers Schedule and on this HAPDP Retention Schedule, except as approved in advance and in writing by a UC Monitor.

Budget: _____

Please attach details – a written justification and breakdown is required for any budget over $25,000. UC will not reimburse unbudgeted work, nor work performed in excess of the budget. Budget revisions must be approved in advance and in writing by a UC Monitor with budget approval authority, following consultation with the Client/Sponsor.

Accepted and Approved:

_____
Name: **("Supervising Attorney")**
Title: ☐ **Chief Campus Counsel** ☐ **Deputy General Counsel**
*The Regents of the University of California-***Office of the President**

_____
Name:
Title:
Firm:

ATTACHMENT 2

University of California Outside Counsel Billing Guidelines

Contents

All invoices need to be submitted electronically. Physical invoices will not be accepted.

A penalty of 5 percent of the invoice's total value will be applied to all invoices submitted 60 days after the due date. An additional 5 percent will be applied to invoices submitted between 90 and 120 days after the due date. Invoices submitted 120 or more days after the due date will not be accepted.

Alternative Fee Arrangements
University of California (UC) cannot process payment without an invoice. Therefore, firms will still need to submit invoices for alternative fee arrangements, even when the arrangement appears on its face to be self-executing.

Hourly Arrangements
Absent an alternative invoicing schedule approved in writing by the monitoring UC attorney, invoices for work completed during a calendar month are due by the end of the following calendar month, including final invoices. All invoices for work performed during UC's fiscal year (July 1st through June 30th) must be received no later than July 15th.

UC will not pay for the following:

A. Timekeepers that are not:
    a. Approved by the monitoring UC attorney *before* they begin work (in exceptional circumstances documented in writing, the monitoring UC attorney may provide post-hoc approval).
    b. Direct employees of the firm (i.e., subcontractors). Work of non-employees may only be billed as expenses.
B. Unapproved rate increases
    a. Increase requests must be submitted to our billing department for review with a business justification at least 60 days before they are proposed to be effective.

b. Approved rate increases are *not retroactive*. New rates are only applicable to future retentions, not existing or panel retentions, unless specified in the applicable retention letter.

C. Time spent due to staffing inefficiencies caused by a change or departure of a firm's personnel
D. Consistent billing of more than eight hours in a day, or more than 150 hours per month, for a timekeeper without justification (trial and immediate pretrial preparation excluded)
E. Overtime charges
F. Commuting time or any other travel time not spent performing University business
G. Clerical, secretarial, and administrative work, regardless of who performs it, including but not limited to: case administration, scheduling, budget preparation, conflicts clearance procedures, data organization
H. Multiple billers for a single task or event
I. Basic legal research – please indicate in the line item description when research is requested by the monitoring UC attorney.
J. Development or drafting of internal research memos or other material attorney work product that is not requested, approved by, or produced to the monitoring UC attorney or other supervising attorney(s)
K. Vague line item descriptions like "attend meeting", "participate in client call", "trial preparation", "research", etc. – Required level of description: "Telephone call with J. Smith and J. Doe re: oral argument preparation".
L. Time spent working with UC or state auditors

Expenses

UC will only pay the actual cost of expenses. Markups are prohibited and will not be reimbursed.

Firms must have the monitoring UC attorney's written approval before retaining a third party vendor or consultant (e.g., experts, mediators, court reporters, subcontractors, eDiscovery vendor). Third party vendor invoices less than or equal to $5,000 will be paid by the law firm and rebilled to UC.

All expenses over $75 require a receipt or invoice copy directly from the vendor attached to the invoice submission. Credit card statements will *not* be accepted.

UC will pay for new technology when it is installed and utilized expressly and solely for UC's benefit. Prior written approval from the monitoring UC attorney is required, along with a certification that the purchase will be made consistent with applicable law and UC policy governing procurement and competitive bidding processes.

Disallowed expenses

A. Overhead expenses
B. Routine postage expenses – Any necessary postage charges (certified mail, overnight service, or oversized packages) must include an explanation and to/from addresses.
C. Any library related expense, including but not limited to LexisNexis, Westlaw, AI-assisted legal practice tools, or other database legal research expenses
D. Billing more than once for documents which are reproduced for multiple witnesses, such as subpoenas

E. Expenses derived from overtime (i.e., transportation or meals)
F. Photocopying (B&W and color)
G. Billing software charges
H. Meals unrelated to overnight travel
I. Private car services or taxi fares (including rideshare services) when more economical options are possible
J. Interest charges

Travel

The following is in accordance with UC's travel guidelines (Policy G-28). Please be as frugal as possible. UC reserves the right to adjust any travel expenses in excess of UC's travel guidelines.

A. All travel (local or out of town) must be preapproved by the monitoring UC attorney. Out-of-town travel requests must be accompanied by justification, including an explanation of why videoconferencing or other telecommunications options are not feasible or appropriate.
B. UC will only pay for time spent explicitly working on UC business during out of town travel.
C. Travel expenses should identify the person who traveled and the reason for the travel (e.g. "Airline ticket to San Diego for Jane Smith to attend 12/02 court hearing").
D. Mileage will be reimbursed at the current IRS rate. Please indicate the number of miles driven.
E. UC will not pay for rental car and airfare higher than economy or coach rates. Basic baggage and ticketing fees are permitted when accompanied by appropriate justification.
F. The following overnight travel expenses are disallowed:
    a. Nightly hotel rate greater than $275 before taxes and mandatory hotel fees
    b. In flight, hotel, or other third party WiFi charges
    c. Meal costs exceeding the then-current UC travel meal allowance
    d. Alcohol or any other entertainment expenses

Audits

UC retains the right to audit all files related to any past invoice. Within reason, the firm will produce any documentation that would support invoices submitted and provide contact information for any individual who submitted invoices on behalf of the firm, would have knowledge regarding any billing, or could answer any or all questions regarding invoices. UC may utilize its own personnel or a UC designated third party to perform such audits. Firms should expect the possibility of the California State Auditor contacting them for audit related questions.

Any billing questions, including payment statuses or short pay inquiries, should be directed to legalbilling@ucop.edu for all other matters.

The monitoring UC attorney must be included on all correspondence with campus departments and aware of all tasks being completed.

UNIVERSITY OF CALIFORNIA

ATTACHMENT 3

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 Firm Name ("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 wishes to disclose PHI to BA. 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 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 provided for 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 information.

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, 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 information.

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 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**
	_____
	Firm Name
_____	_____
(Signature)	(Signature)
_____	_____
Name, Title	Name, Title
_____	_____
(Date)	(Date)

ATTACHMENT 4

UC Legal Health Affairs, Privacy & Data Protection Law 2025-27 Preferred Provider Program Request for Proposals

RFP Overview

The University of California, UC Legal - Office of the General Counsel ("UC Legal") seeks a limited number of preferred outside law firms to assist with the majority of our health law, privacy, and cybersecurity matters. The types of matters included in this Request for Proposals ("RFP") are outlined in the Scope section below (collectively, the "Covered Matters"). The firms we ultimately select will be known as the UC Legal Health Affairs, Privacy & Data Protection Counsel preferred provider panel and will represent the University as part of the UC Legal Health Affairs, Privacy & Data Protection Law Preferred Provider Program ("Panel"). We anticipate that each firm will have significant opportunities, subject to performance, to represent the University. While a separate litigation panel has been selected by our Litigation section, UC Legal practice groups work closely on many non-litigated and litigated matters.

Panel firms will be able to represent the University across all Covered Matters for which they have qualified and may have the opportunity to bid for work in other practice areas not indicated in the Scope section below. Although we reserve the right to assign Covered Matters work to non-Panel firms, we anticipate that a significant majority of the Covered Matters work will go to Panel firms.

Responding firms must agree to abide by the Panel Requirements and Terms and Conditions of this RFP as stated below.

About UC

The University of California, one of the largest and most acclaimed institutions of higher learning in the world, is dedicated to excellence in teaching, research, health care, and public service. It is a public institution encompassing ten undergraduate and graduate campuses, six academic medical centers, eight community hospitals, twenty health professions schools, and a statewide Division of Agriculture and Natural Resources. The University also is involved in the operation and management of three national laboratories for the U.S. Department of Energy.

The Office of the President, based in Oakland, California, provides system-wide management of the University. Its divisions oversee UC's academic mission, budget, external relations, legal matters, and business and financial activities. The University is governed by a Board of Regents.

About UC Legal

UC Legal, working collaboratively with our clients, seeks to advance the University's mission through skilled advice, vigorous advocacy, and effective, proactive counsel. Our goal is to be valued and trusted partners, recognized for our creativity, industry-leading expertise, and commitment to client objectives. We are committed to fairness and diversity in all our interactions, and we value a commitment to diversity in our retained counsel. For more information about us and our values, please visit our website at https://www.ucop.edu/uc-legal.

UC Legal attorneys, whether located at the Office of the President or resident at the University's campuses, medical centers, and national laboratories, partner with outside counsel to provide legal services in a variety of areas. Covered Matters arising out of this RFP typically will be supervised by Oakland-based attorneys in UC Legal's Health Affairs, Privacy & Data Protection ("HAPDP") section. Other sections of UC Legal supervise matters in Legal Policy and Operations; Business, Transactions & Innovation; Education Affairs, Employment & Governance; and Litigation. Smaller matters sometimes are supervised locally at a campus, medical center, or national laboratory.

Panel Scope (Covered Matters)

The scope of this RFP and the Panel is, except as otherwise expressly provided, for U.S. matters only, which are heavily concentrated in California. The matter types are broken into two groups:

- Group I matters are typically complex matters that pose a significant operational, reputational, and/or financial risk to the university system and that involve anticipated outside counsel spend exceeding $100,000 per matter. Group I matters include complex corporate transactions (e.g., whole hospital mergers, acquisitions, or affiliations; multi-year system-wide provider agreements with health plans; ancillary provider joint ventures; single-campus health plan agreements). Additionally, Group I matters are those that require legal expertise on regulatory, white collar (including both health, privacy, data protection and research investigations), and/or cybersecurity issues.

- Group II matters are highly specialized and typically (but not consistently) involve lower outside counsel spend (i.e., less than $100,000 per matter). The smaller size of these matters may include fixed-fee retainers for routine advisory work.

You may choose to apply to represent the University in any or all of the matter types listed, but you should apply only for areas in which you have demonstrated expertise (in both substance and risk level) and for which you can offer economically practical services. Please respond to the questions for each matter type for which your firm would like to be considered.

Group I (complex regulatory, white collar or cybersecurity matters; complex corporate transactions)

- Cybersecurity Advice, Breach Response and Notification
- Reimbursement/Payer Disputes (commercial and government payers with UC as the provider in the dispute)
- Transactions
- White Collar – Internal Investigations and Defense of Government Investigations (including via *qui tam* complaints and/or Congressional investigations and including in the areas of health, cybersecurity and research such as foreign influence, export control, research security or Higher Education Act Section 117 investigations)

Group II (highly specialized, typically smaller, less frequent – but sometimes high-impact/high-risk; deep knowledge of both federal and California regulatory systems generally required)

- Academic Affairs
  - Faculty-Administration Relations/Shared Governance
  - Faculty Practice Plans (and affiliations with Academic Health Systems)
  - Graduate Medical Education including academic affiliations, accreditation surveys, reimbursement, investigations, moonlighting rules, etc.
  - Religious Liberty/Establishment Issues
- Antitrust (healthcare-specific) including but not limited to:
  - Office of Health Care Affordability (OHCA) Cost and Market Impact Review (CMIR)
  - California Attorney General Nonprofit Transaction Review
- Health Insurance/Health Plans (employer and provider sides)
  - Captive Insurers; Risk Retention Groups
  - Managed Care/Insurance Contracting
  - Managed Care/Insurance Regulation (esp. Knox-Keene; DMHC; CDI)
  - Self-Funded Health Plan Administration
- Information Privacy, Confidentiality, and Security
  - Cybersecurity, Breach Response and Notification
  - AI and "Big Data" including best practices with respect to sharing of de-identified data
  - Federal privacy laws and regulations including HIPAA, FERPA, GLBA, CIRCIA, SAMHSA Regulations, human subjects research laws and regulations promulgated by OHRP and FDA, interoperability and information blocking regulations, and related higher education, research, and federal health privacy rules
  - Federal information security laws including HIPAA and FISMA, standards including NIST and ISO, and related higher education, research, and health privacy rules
  - California privacy and security laws and regulations including the Information Practices Act, Confidentiality of Medical Information Act, and other California health privacy rules
  - National and international data breach reporting rules
  - The European Union's General Data Protection Regulation and the EU AI Act
  - Other international privacy and security laws and regulations
  - *If you are applying for this work, please describe any internal technical experts you employ, specify whether they are attorneys or non-attorneys, and provide their rates*
- Medical Staff
  - PSQIA
  - Medical Staff Governance
  - Peer Review including Fair Hearings, whether involving academic medical centers, community hospitals or student health centers and whether on behalf of the medical staff or as hearing or appeals officer. Please also describe your expertise in advising the medical staff on (1) potential litigation claims under Cal. Health & Safety Code 1278.5, and (2) the impact of parallel investigations or hearings in faculty discipline, Title IX, etc. Please note that this panel does not encompass actual litigation under Section 1278.5 or matters involving faculty discipline, Title IX, etc.

- Pharmacy Regulation
  - Hospital, Retail and Clinic Pharmacy Representation before Board of Pharmacy
  - Controlled substances laws and regulations
  - Pharmacy laws and regulations including licensing and compounding pharmacy rules
- Public/Academic and Community Hospital and Health System Operations and Reimbursement
  - California Medical Foundations (including Cal. Health & Safety Code 1206(l))
  - Clinical Laboratories – State and Federal Accreditation and Reimbursement
  - Enrollment (Medicare, Medicaid/Medi-Cal)
  - FQHCs (Federally Qualified Health Centers)
  - Government Health Care Program Reimbursement (including Medicare, California Waiver/Medi-Cal and Supplemental Payment Systems; Intergovernmental Transfers; Certified Public Expenditures)
  - Hospital Operations/Regulatory Advice (e.g., CCR Title 22, Medicare COPs, TJC, LPS Act)
  - Licensure and Accreditation including change of ownership situations
  - Nonprofit Tax Matters
  - VAMC Affiliations
- Regulatory/Internal Investigations/White Collar
  - Conflicts of Interest/Open Payments
  - Controlled Substances Regulation and Diversion
  - Corporate Governance (with particular focus in public entities, higher education, and/or health care organizations)
  - Fraud and Abuse – Health Care
  - Fraud and Abuse – Research
  - Government Investigations/Audits (e.g., DOJ, OIG, NIH, NSF, OHRP, FDA, CDPH, CMS)
  - Immigration
  - Medical Marijuana/Legalization
  - Sexual Harassment/Sexual Violence in Academic Medical Centers
  - Use of Civil False Claims Act to Sue on the Basis of Inaccurate Cybersecurity Representations including to Federal Agencies
  - Anti-Discrimination in Academic Medical Centers, e.g., Title VI and Section 1557 Compliance
  - Self-disclosures (e.g. DHCS, OIG, SRDP)
- Research and Clinical Trials
  - Animal Research
  - Conflicts of Interest in Research (including NIH, NSF, NASA, DOE, FDA regulations, and undue foreign influence matters)
  - Export Controls/Fundamental Research Exclusion/OFAC Sanctions
  - FDA Regulation of Drugs, Devices, and Biologics
  - Grants and Contracts (government and nongovernment sponsors)/OMB Uniform Guidance/Research Terms and Conditions/Cost Principles

  - Human Subjects Research/Clinical Trials
  - Research and Health Data – ownership, access, data sharing requirements
  - Research Compliance (Miscellaneous)
  - Research Misconduct/Research Integrity Compliance and Investigations (and PHS and NSF regulation)
  - VAMC/VA Research Affiliates
- Transactions/Corporate (specific to healthcare and research)
  - Government Contracts/Federal Acquisition Regulation
  - Group Purchasing Organizations
  - International (specify regions/countries and for each, whether services are provided directly by your firm or by firm partners or affiliates)
  - Mergers/Acquisitions/Joint Ventures/Clinically Integrated Networks
  - Procurement; Public Contracts/Public Bidding (California)
  - Public Entity Affiliations with Health Systems with Ethical and Religious Directives
  - Venture Investment/Finance

Panel Requirements

1. Abide by the Health Affairs, Privacy & Data Protection Master Retention (Appendix A); the UC Legal Outside Counsel Guidelines (Appendix B); where applicable, the Business Associate Agreement (Appendix C); and the University's Appendix Data-Security (Appendix D)*
2. Confirm that no conflicts exist (or in response to the General Questions below, specify any that do), and agree that with very limited and narrow exceptions proposals for which must be made as part of your RFP response, UC Legal will not approve advance blanket waiver requests and instead will consider all waivers on a case-by-case basis
3. For Group I matters, please propose value-based pricing methodologies that would be acceptable to your firm (see Value-Based Pricing section below)
4. For Group II matters only, provide a proposal for a heavily discounted monthly retainer for routine advice in any combination of the practice areas listed (all-in, by group, or individually)
5. Please provide an additional annual volume-based discount based on annual spend on your firm across HAPDP and/or across all areas of UC Legal
6. Use the UC eBilling system for electronic invoice submittals (CounselLink)
7. Participate in the Annual Performance Review (see Annual Performance Review section below)
8. Participate, as requested by UC, in reporting and other activities related to diversity, equity, inclusion and belonging
9. No mention of the University of California or use of its marks in any marketing or similar material without prior written approval and then only consistent with the requirements of Cal. Ed. Code §§ 92000 et seq. and applicable University policies
10. Provide at least a 15% discount for any hourly fees (hourly work performed only with prior approval) and state the percentage discount that you are offering

---

* The current master retention letter and outside counsel guidelines are attached.

Matter Engagement Process

For most Group I matters in which we intend to engage outside counsel, those firms that have been qualified for that matter type will be given a matter-specific RFP which will include a summary of the matter, copies of relevant materials, a few substantive questions about the specific matter as well as request a list of the attorneys who are proposed to work on it. In addition, the firm will submit either a pricing template or other requested pricing structure with a proposed value-based pricing proposal. We will review the proposals and select a firm to represent the University in that matter. Selection will be weighted heavily on the substantive responses, but the proposed pricing certainly will be a factor, as will the composition of the proposed team. Although from time to time these Group I matter-specific RFPs may also include a non-Panel firm as a recipient of those RFPs, these RFPs will be sent primarily to Panel firms and Panel qualification will be a significant positive factor in awarding these RFPs.

Annual Performance Review

As a means to enhance communication and provide feedback to Panel firms, UC Legal may, at its discretion and as necessary, schedule an annual performance review with each Panel firm at the UC Legal office in Oakland or via videoconference at the firm's discretion. We may request that the Panel relationship partner(s) attend. Attendees from UC Legal may include the General Counsel, Deputy General Counsel and Managing Counsels of HAPDP, other UC Legal lawyers, and/or representatives from our clients. The annual performance review will include a review of the matters, substantive issues, results, financials, and any other topics requested by either party. Panel firms will not charge for time or expenses to attend the annual performance review. Results of these reviews may influence continued participation in the Panel.

Engagement Requirements

Upon acceptance into the Panel, UC Legal will provide selected firms with an engagement letter indicating agreement to abide by the Panel Requirements and Terms and Conditions as stated in this RFP. After the engagement letters are signed and approved, each subsequent matter assigned to a Panel firm under the Panel will require only an approved Retention Schedule and a reference to the approved engagement letter (including Business Associate Agreement and Appendix-Data Security).

General Questions – Responses Required

Please provide succinct responses within Smartsheet that clearly and directly answer each question below. Smartsheet has a 4,000 character limit, including spaces.

1. **Contact Information/Relationship Partner(s).** Provide the name and contact information of the attorney with primary responsibility for the overall relationship with UC Legal (note: more than one attorney may be named; for example, if you are the relationship partner for the Litigation Team, you may name a different relationship partner for the Health Affairs, Privacy & Data Protection Team, and within HAPDP, you may name more than one relationship partner – e.g., one for transactional matters and one for regulatory matters or one for California and one for Washington, DC/Federal matters).

2. **Firm/Office Demographics.** *The following information will not affect evaluation of a firm's application*. Please provide the following information (you may attach your current NALP form to this application if the information requested is contained therein, but all points below must be addressed in your response):
    - Location of offices
    - Number of attorneys firm wide and number in California offices by location
    - Number of equity partners/members, non-equity partners/members, associates, counsel, non-traditional track/staff attorneys, and summer associates in total and in each NALP-designated population (gender identity, race/ethnicity, disability status, openly LGBTQ, and military veterans)
    - Number of new "homegrown partners" (i.e., associates in U.S. offices who were promoted to partner within the past three years) in total and in each NALP-designated population (gender identity, race/ethnicity, disability status, openly LGBTQ, and military veterans)
    - The name and contact information for your diversity chair

3. **Recruitment/Hiring Practices.** Please provide the following:
    - Information about your firm's recruitment practices and how they address historic underutilization of NALP-designated populations
    - Information about diversity fellowships or scholarships offered by your firm
    - Information about any other initiatives sponsored or supported by your firm aimed at promoting diversity within your firm, both generally and in leadership positions, or in the profession
    - Information about any other initiatives sponsored or supported specifically by the proposed relationship partner(s) identified in your response to Question No. 1 aimed at promoting diversity within your firm or in the profession

4. **UC Matters.** Describe how UC matters and credit for working on UC matters are assigned to partners, associates, and other staff.

5. **Scenario.** During a client conference, an equity partner makes sexist, culturally insensitive, racist, homophobic, ableist, or otherwise discriminatory remarks. How would the firm handle the situation? Please include descriptions of any policies and procedures, committees, or trainings currently in place at the firm that would apply to this situation.

6. **Diversity Efforts.** Describe where you think your firm needs to improve the most in creating a more diverse, equitable, and inclusive workplace.

7. **Program/Matter/Knowledge Management.** Describe your firm's processes and systems for both program and knowledge management, and explain how these processes and systems will be used to benefit UC Legal. These may range from client extranets to billing/reimbursement dashboards to access to educational presentations, for example.

8. **Personal Conflicts of Interest.** Describe any business or personal relationships (other than through the University) your firm or proposed members of your panel team have

with any UC Legal attorney or staff member, or with other senior leaders of the University of California or UC Health (e.g., Board of Regents, Regents committee members, Regents Officers, President, Vice Presidents, Chancellors, Vice Chancellors, Deans, CEOs, CFOs, CMOs, COOs, CSOs).

9. **Value-Added Services.** Describe any additional services that you would provide UC Legal at no cost to enhance the value of your service overall (e.g., in-service training, access to extranets, etc.). Please also describe your willingness to provide complimentary legal advice on short questions (e.g., 3 to 5 conversations of 15 minutes or less per quarter) and whether that willingness would depend on annual outside counsel spend, volume or frequency of questions, or other factors.

10. **Budgeting and Performance.** Describe any practices, mechanisms or tools you use to assist with budgeting on matters. Please describe how you would communicate with the University when spend on a matter approaches thresholds of total estimated budget or a fixed fee (e.g., 50% or 75% or 90%) and how you would provide early notice of a need to augment the estimated budget or attempt to renegotiate a fixed fee. Given that you are not permitted to exceed estimated budget or a fixed fee without prior written approval by your UC Legal monitor, please describe your willingness to write off unapproved billed time exceeding the estimated budget or a fixed fee. Please also describe the circumstances when you would write off billed time for a timekeeper that the University believes has not provided high-quality legal services or has other performance issues.

11. **Firm Conflicts.** Describe any conflicts your firm has with the University as a result of your representation of other clients for which you will require a waiver (e.g., as a result of pending litigation or transactions). Also describe any (narrowly tailored) blanket or future waivers you would like us to consider should we choose you for our panel.

12. **Ethical Walls.** Describe the arrangements you are willing and able to make to assure that confidential client information is not inadvertently released or otherwise utilized when the University has waived a conflict.

13. **Information Security.** For any firm bidding for Group I matters, please provide a detailed description of your security controls pursuant to a formally recognized framework, such as HECVAT, HITRUST, or SOC2. Due to space limitations with SmartSheet, we ask that you submit this documentation in a separate email to Michael.Gormley@ucop.edu with the subject reference "Q13 - [Firm Name] HAPDP Group I." If selected pursuant to our initial assessment, we may ask to confer with members of your organization to discuss your information security plan and to review any third-party assessments of your security controls. Because Group I matters involve proprietary, confidential, and sensitive data, firms bidding for Group I matters will be required to include Appendix D (the Appendix Data Security) as part of their panel engagement letter. Firms bidding only for Group II matters may submit a description of their security controls as part of their initial proposal (sent in a separate email) or submit such documentation upon request by HAPDP. In order to be approved to the Panel, every firm, including those bidding for Group II matters, must provide acceptable security documentation. Firms handling Group II matters which involves processing

sensitive data may also be required to include Appendix D as part of their panel engagement letter. Firms handling Group II matters which do not involve processing sensitive data will not be required to include Appendix D as part of their panel engagement letter.

14. **Use of Artificial Intelligence (AI).** Describe how your firm utilizes AI in each practice area where you are applying. Be as specific as possible, including any specific AI tools (including off-the-shelf tools that are customized by the firm) that are used and how they are customized or integrated into workflows and in particular if and how AI is used for (1) legal research, (2) e-discovery, (3) contract and/or policy drafting or negotiating, (4) drafting of legal advice, (5) billing, (6) presentations whether related to particular projects or for CLE or client pitches, (7) client communications and (8) responses to panel applications such as this one or RFP responses for particular matters. If your firm has a policy for the use of AI in specific cases, practices areas, or overall, please describe this policy, including whether the firm permits use of personal accounts created in generative AI tools, whether the firm permits use of client materials (de-identified or containing privileged materials or containing PII or PHI) in training or use of AI, whether the firm discloses to clients when generative AI is used in their legal or administrative matters, and whether any human review is required before any materials drafted through generative AI are sent externally or relied upon. How does the firm monitor compliance by its attorneys and staff of any firm policies regarding AI use? If the firm contracts for the use of AI as an item or service, how will you ensure the panel requirements are passed onto these vendors? Will your firm adhere to any client policies or requests regarding the use of AI? If your firm utilizes AI for a given practice area, describe any additional costs and/or savings that are passed on to your clients for such use, how such fees are determined, any training provided to attorneys and staff of in the use of AI, any allotment of hours provided to attorneys or staff to learn how to use AI, and steps your firm takes in mitigating any risk associated with the use of AI.

15. **Value-Based Pricing/Alternative Fee Arrangements.** Describe your experience with value-based pricing and other alternative fee arrangements in each area where you are applying. Be as specific as possible. A general "we are open to alternative fee arrangements" or "we have worked under alternative fee arrangements" is not a useful response.

16. **Hourly Rates.** For situations where UC Legal approves hourly work, please provide your current rack rates and rates expected for CY 2025-27 for all attorneys and other billing staff you propose to work on Panel matters. Also provide your proposed hourly rate for partners, senior counsel/of-counsel, associates, and non-attorney billing staff (e.g., paralegals and crisis communications experts). We strongly prefer standardized rates in each class but will accept proposals by practice group or, if absolutely necessary, by individual. *Provide a proposal that will be good for at least three years (whether one fee good for the entire period or a fee plus a defined escalator).*

17. **Professional Misconduct/Professional Malpractice.** Has your firm or any firm attorney been a named defendant in a legal malpractice case during the past 10 years, or has any firm attorney been sanctioned by a court or regulatory authority or otherwise

disciplined by any state Bar? If so, please provide details.

18. **Major Expected Changes.** Describe any potential or planned changes that, in the next 12-24 months, could significantly change any of the information provided in your response to this RFP.

19. **Additional Considerations.** Discuss any other issues or considerations that you believe are relevant as a candidate for the Panel.

Group-Specific Questions – Responses Required

For each matter group or specific matter type for which you wish to be considered in Group I, please provide:

1. A brief description of your relevant practice and how this practice differentiates itself from similar practices at other firms.

2. The name, contact information and background information of the attorney proposed to have primary responsibility for the specific area of practice for UC as well as of all other members of the proposed team. Explain why each individual has been proposed and their specific area of work or specialty, including any relevant experience with government agencies regulating health care, academic research or teaching, or cybersecurity.

3. A description of at least three similar matters handled in the past year along with the final disposition as applicable. For Group I matters related to cyber incident response, please also describe your firm's use of data mining tools or advanced analytics to aide/expedite the assessment of files for reportable data elements (e.g., financial account information, Social Security Numbers, dates of birth, etc.).

For Group II matters, please respond to at least the first two questions.

Terms and Conditions

Applications must be submitted through the Smartsheet form available at https://www.ucop.edu/uc-legal/hatl-rfp.html. We strongly recommend preparing your responses before filling out the submission form in Smartsheet. Smartsheet does not have an option to save your progress through multiple sessions. UC Legal will accept submissions **no later than 5:00 p.m. on Friday, November 15, 2024.**

We do not intend to look at extraneous marketing material during this process. **ALSO, DO NOT SEND PAPER. IT WILL BE RECYCLED WITHOUT REVIEW AND ITS CONTENT WILL NOT BE CONSIDERED IN THIS PROCESS. WE LIKE THE TREES AND DO WHAT WE CAN TO SAVE THEM.**

All information provided by UC Legal in connection with this RFP shall be considered proprietary information of UC Legal. All documentation and/or ideas submitted by your firm shall also become the property of UC Legal.

If your firm has a question during this process, please send it to Michael.Gormley@ucop.edu. All such questions or requests must be received by 5:00 p.m. on November 15, 2024, and all such questions or requests received after such date will be answered, if at all, by UC Legal, in its sole discretion. FAQs regarding the University of California 2025-27 HAPDP panel can be found at: 2025-27 HAPDP Panel FAQs. You are not authorized to contact any other University employee concerning this RFP. Failure to adhere to this requirement will be grounds for disqualifying your proposal.

Following review of the written proposals, UC Legal may ask firms in which it continues to have an interest to participate in an interview by videoconference. In no event will UC Legal schedule meetings in advance of receipt of your RFP response, and the only meetings UC Legal intends to hold, if any, are with the finalist law firms. In no event should any firm bill any time in connection with the videoconference interview or in preparation of any materials in response to this RFP. If your firm is invited to an interview, only the individuals being proposed to work as part of the Panel should attend. This means, for example, that you should not send an employment lawyer to represent your firm on the HAPDP Panel just because that person happens to have a pre-existing relationship with the University; doing so will be counterproductive. UC Legal also may award a position as a Preferred HAPDP Counsel without further negotiations or discussions or further interviews with any given finalist law firm.

This RFP does not bind UC Legal to any obligations or impose liability for any costs or expenses incurred by your firm in responding to the proposal or traveling to an interview in connection with this RFP. UC Legal, in its sole discretion, may or may not make an award and reserves the right to reject any and all responses received. UC Legal also reserves the right to terminate a retention at any time in its sole discretion.

Evaluation Criteria

UC Legal will award the matter to the bidder(s) in its sole discretion based upon a combination of experience, expertise, demonstrated commitment to diversity, proposed team, and the greatest overall value.

Appendices

Appendix A: Health Affairs, Privacy & Data Protection Law Group Master Retention

Appendix B: UC Legal Outside Counsel Guidelines and Billing Submission Guidelines

Appendix C: UC Legal Business Associate Agreement

Appendix D: Appendix- Data Security

ATTACHMENT 5

ARTICLE 1. PURPOSE AND INTRODUCTION

A. In the course of providing the Goods and/or Services contemplated by the Agreement, Supplier may gain access to the University of California's (UC) Institutional Information and/or IT Resources (both defined below). In such an event, UC and Supplier desire to appropriately protect Institutional Information and IT Resources. The purpose of this Appendix-Data Security is to specify Supplier's cybersecurity and risk management responsibilities when Supplierhas access to Institutional Information and/or IT Resources.

B. Any capitalized terms used here have the meaning ascribed to such terms as set forth in the Agreement or Incorporated Documents.

C. Supplier must provide commercially acceptable cybersecurity and cyber risk management to protect Institutional Information and/or IT Resources. This must include, but is not limited to the Supplier:

1. Developing and documenting a plan that protects Institutional Information and IT Resources.
   - Supplier must responsibly execute this plan.
   - Supplier's approach must conform to a recognized cybersecurity framework designed for that purpose.[1]
   - Supplier's information security plan must be supported by a third-party review or certification. Supplier may only use an alternative to a third- party review if approved by the responsible UC Information Security Officer.

2. Conducting an accurate and thorough assessment of the potential risks to and vulnerabilities of the security of the Institutional Information and/or IT Resources. Supplier must mitigate anticipated risks effectively. This includes implementing commercially acceptable security policies, procedures, and practices that protect Institutional Information and/or IT Resources.

3. Updating its plan to effectively address new cybersecurity risks.

4. Complying with pertinent contractual and regulatory responsibilities.

5. Providing UC with evidence of compliance with Supplier's information security plan.

6. Keeping UC informed with timely updates on risks, vulnerabilities, Security Incidents, and Breaches.

7. Keeping UC informed of any measures UC must perform to ensure the security of Institutional Information and IT Resources.

[1] Examples include the latest versions of PCI DSS, NIST CSF, CIS Critical Security Controls, IS0 27000 series, NIST SP 800-53 and NIST SP 800-171.

D. If, in the course of providing the Goods and/or Services under the Agreement, Supplier engages in transactions with UC affiliated individuals (including but not limited to: students, staff, faculty, customers, patients, guests, volunteers, visitors, research subjects, etc.), as a benefit and result of the Agreement, Supplier must treat any data about UC affiliated individuals that Supplier creates, receives, and/or collects in the course of those transactions with the same level of privacy and security protections and standards as required of Institutional Information by this Appendix.

E. Supplier agrees to be bound by the obligations set forth in this Appendix. To the extent applicable, Supplier also agrees to impose, by written contract, the same terms and conditions contained in this Appendix on any sub-supplier retained by Supplier to provide or assist in providing the Goods and/or Services to UC.

F. To the extent that a requirement of this Appendix conflicts with those of any other UC Agreement or Incorporated Document, the most stringent requirement (including but not limited to: least risk to UC, shortest time, best practice, etc.) will apply.

ARTICLE 2. DEFINED TERMS

A. "Breach" means: (1) Any disclosure of Institutional Information to an unauthorized party or in an unlawful manner; (2) Unauthorized or unlawful acquisition of information that compromises the security, confidentiality, or integrity of Institutional Information and/or IT Resources; or (3) The acquisition, access, use, or disclosure of protected health information (PHI) or medical information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) or California law.

B. "Illicit Code" means: (1) Any code UC would not reasonably expect to be present or operating; (2) Hidden software or functionality with adverse or undesired actions or consequences; (3) Code that replicates or transmits Institutional Information or activates operating systems or other similar services without the express knowledge and approval of UC; (4) Code that alters, damages, or erases any Institutional Information or software without the express knowledge and approval of UC; or (5) Code or apparatus that functions in any way as a: key lock, node lock, time-out, "back door," "trap door," "booby trap," "dead drop device," "data scrambling device," or other function, regardless of how it is implemented, which is intended to alter or restrict the use of or access to any Institutional Information and/or IT Resources.

C. "Institutional Information" means: Any information or data created,received, and/or collected by UC or on its behalf, including but not limited to: application logs, metadata, and data derived from such data.

D. "IT Resource" means: IT infrastructure, cloud services, software, and/or hardware with computing and/or networking capability that is Supplier owned/managed or UC- owned, or a personally owned device that stores Institutional Information, is connected to UC systems, is connected to UC networks, or is used for UC business. IT Resources include, but are not limited to: personal and mobile computing systems and devices,

mobile phones, printers, network devices, industrial control systems (including but not limited to: SCADA, PLCs, DPC, Operational Technology, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens, or Internet of Things (IoT).

E. "Major Change" means: The implementation of a change that could have an effect on the security of an IT Resource or Institutional Information. The scope includes changes to architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items. These include changes related to:

1. Technology upgrades or migrations.
2. Responses to Security Incidents.
3. Modifications of scope (data elements, features, location of Institutional Information, etc.).
4. Regulatory guidance.
5. Law and legal regulations.
6. Responses to risk assessments.
7. Addressing vulnerabilities.
8. Material updates or shifts in technologies used by Supplier.

F. "Security Incident" means: (1) A material compromise of the confidentiality, integrity, or availability of Institutional Information; (2) A single event or a series of unwanted or unexpected events that has a significant probability of compromising UC business operations or threatening Institutional Information and/or IT Resources; (3) Any event involving a cyber intrusion; or (4) A material failure of Supplier's administrative, technical, or physical controls that resulted or could have resulted in an adverse impact to the confidentiality, integrity, or availability of Institutional Information or IT Resources.

ARTICLE 3. ACCESS TO INSTITUTIONAL INFORMATION AND IT RESOURCES

A. Supplier must limit its access to, use of, and disclosure of Institutional Information and IT Resources to the least invasive degree necessary required to provide the Goods and/or Services.

1. Supplier may not access or use Institutional Information and IT Resources for any purpose except to provide the Goods and/or Services.
2. For the avoidance of doubt, Supplier may not access, use, or disclose Institutional Information and IT Resources outside the scope of the Agreement for purposes of, including but not limited to: marketing, advertising, research, sale, or licensing unless expressly approved in writing by UC.

B. In the event that Goods and/or Services include the review of a specific Security Incident or a threat to or anomaly in Institutional Information or IT Resources, Supplier must limit inspection to the least invasive degree necessary required to perform the investigation.

ARTICLE 4. SUPPLIER'S INFORMATION SECURITY PLAN AND RESPONSIBILITIES

A. Supplier acknowledges that UC must comply with information security standards as required by law, regulation, and regulatory guidance, as well as by UC's internal security program that protects Institutional Information and IT Resources.

B. Supplier must establish, maintain, comply with, and responsibly execute its information security plan.

C. Supplier's initial information security plan is attached as Exhibit 2 and incorporated by reference.

D. Updates to Exhibit 2 will occur as follows:

1. On an annual basis, Supplier will review its information security plan, update it as needed, and submit it upon written request by UC.

2. In the event of a Major Change, Supplier will review its information security plan, update it as needed, and submit it to UC as detailed herein.

E. If Supplier makes any material modifications to its information security plan that will affect the security of Institutional Information and IT Resources, Supplier must notify UC within seventy-two (72) calendar hours and identify the changes.

F. Supplier's Information Security Plan must:

1. Ensure the security (including but not limited to: confidentiality, integrity, and availability) of Institutional Information and IT Resources through the use and maintenance of appropriate administrative, technical, and physical controls;

2. Protect against any reasonably anticipated threats or hazards to Institutional Information and IT Resources;

3. Address the risks associated with Supplier having access to Institutional Information and IT Resources;

4. Address applicable regulations and/or external obligations listed in Exhibit 1;

5. Comply with all applicable legal and regulatory requirements for data protection, security, and privacy;

6. Clearly document the cybersecurity responsibilities of each party;

7. Follow UC records retention requirements outlined in the Statement of Work (SOW) or in UC's Terms and Conditions;

8. Prevent the sharing of passwords or authentication secrets that provide access to Institutional Information and/or IT Resources;

9. Prevent the use of passphrases (passwords) or other authentication secrets that are common across customers or multiple unrelated UC sites or units;

10. Prevent unauthorized access to Institutional Information and IT Resources;

11. Prevent unauthorized changes to IT Resources;

12. Prevent the reduction, removal, or turning off of any security control without express written approval from UC;

13. Prevent the creation of new Supplier accounts to access Institutional Information and IT Resources without express written approval from UC;

14. Prevent the storing, harvesting, or passing through of UC credentials (username, password, authentication secret, or other factor); and

15. Prevent the use or copying of Institutional Information for any purpose not authorized under the Agreement or any associated Statement of Work (SOW).

ARTICLE 5. REQUESTS FROM UC AND EVIDENCE OF COMPLIANCE

A. Supplier must provide UC with evidence that demonstrates to UC's reasonable satisfaction Supplier's adherence to its information security plan (including but not limited to: third-party report, attestation signed by an authorized individual, attestation of compliance by a qualified assessor, or a mutually agreed upon equivalent) upon execution of the Agreement, upon reasonable request (including but not limited to: annually, after Major Changes, and/or as a result of a Security Incident), or as required by any applicable regulatory or governmental authority.

B. Supplier must respond to UC's reasonable questions related to cybersecurity controls, Security Incidents, or Major Changes, newly published vulnerabilities, and/or risk assessments within ten (10) business days.

C. UC may request and perform a security audit using a qualified third party or a mutually agreed upon alternative annually or as a result of a Breach.

ARTICLE 6. NOTIFICATION OF MAJOR CHANGES AND VULNERABILITY DISCLOSURES

A. Within twenty (20) business days, Supplier must notify UC regarding changes in Supplier's security posture or IT infrastructure. Such notices must occur:

1. When Major Changes happen.
2. When Supplier becomes aware of a vulnerability that warrants a CVE[2] rating of "High" or "Critical," based on the latest CVE version, for which a patch is not yet available or for which Supplier will delay application of an available patch.

B. Supplier must use commercially acceptable efforts to remediate, within twenty (20) business days, any vulnerability rated as CVE High or Critical.

C. In response to Major Changes, Supplier must update its information security plan no later than fifteen (15) days into the next calendar quarter and must provide updated evidence of compliance with the information security plan.

[2] Common Vulnerabilities and Exposures (CVE) is a dictionary-type list of standardized names for vulnerabilities and other information related to security exposures maintained by The MITRE Corporation. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools. The CVE list can be found at: cve.mitre.org

ARTICLE 7. RETURN AND DISPOSAL OF INSTITUTIONAL INFORMATION

A. Within thirty (30) calendar days of the termination, cancellation, expiration, or other conclusion of the Agreement, Supplier must return all Institutional Information to UC and then dispose of the Institutional Information in possession of Supplier as detailed herein. This provision also applies to all Institutional Information that is in the possession of sub-suppliers or agents of Supplier.

B. Such disposal will be accomplished using the methods described in UC's Institutional Information Disposal Standard (https://security.ucop.edu/policies/institutional-information-disposal.html) or an alternative approved by UC.

C. Supplier will certify in writing to UC that such return and/or disposal has been completed.

D. If Supplier believes that return and/or disposal of Institutional Information is technically impossible or impractical, Supplier must provide UC with a written statement explaining the reason for this conclusion. If UC determines that return and/or disposal is technically impossible or impractical, Supplier will continue to protect the Institutional Information in accordance with the terms of this Appendix for as long as the Institutional Information is in Supplier's possession.

ARTICLE 8. NOTIFICATION OF CORRESPONDENCE CONCERNING INSTITUTIONAL INFORMATION

A. Supplier agrees to notify UC promptly, both orally and in writing, but in no event more than seventy-two (72) calendar hours after Supplier receives correspondence or a complaint that relates to a regulation, contractual obligation, Breach, or material risk concerning Institutional Information. For purposes of this Article 8.A, a correspondence or complaint may include, but is not limited to, any communication that originates from law enforcement, regulatory or governmental agencies, government investigators, corporations, or an individual, but excludes normal customer service correspondence or inquiries.

ARTICLE 9. COORDINATING, REPORTING, AND RESPONDING TO BREACHES AND SECURITY INCIDENTS

A. Reporting of Breach or Security Incident: If Supplier reasonably suspects or confirms a Breach and/or a Security Incident impacting Institutional Information and/or IT Resources, Supplier must promptly notify UC both orally and in writing using the contacts in the Agreement. Supplier must provide such notifications no later than (1) seventy-two (72) calendar hours after the initial suspicion of a Security Incident and/or Breach and (2) seventy-two (72) calendar hours after the initial confirmation of a Security Incident and/or Breach, if Supplier is able to make such a confirmation. Supplier's notification must identify:

1. Contacts for both technical and management coordination;

2. Escalation and identifying information, such as ticket numbers, system identifiers, etc.;
3. The nature of the Breach and/or Security Incident;
4. The Institutional Information and/or IT Resources affected;
5. What Supplier has done or will do to mitigate any deleterious effect; and
6. What corrective action Supplier has taken or will take to prevent future Security Incidents.

B. Supplier will provide other information as reasonably requested by UC.

C. In the event of a suspected Breach and/or Security Incident, Supplier will keep UC informed regularly of the progress of its investigation until the incident is resolved.

D. Coordination of Breach Response or Security Incident Activities: Supplier will fully cooperate with UC's investigation of any Breach and/or Security Incident involving Supplier and/or Goods and/or Services. Supplier's full cooperation will include, but not be limited to, Supplier:

1. Promptly preserving any potential forensic evidence relating to the Breach and/or Security Incident;
2. Remedying the Breach and/or Security Incident as quickly as circumstances permit;
3. Promptly, but no more than seventy-two (72) calendar hours after the discovery of Breach and/or Security Incident, designating a contact person to whom UC will direct inquiries and who will communicate Supplier responses to UC inquiries;
4. As rapidly as circumstances permit, assigning/using appropriate resources to remedy, investigate, and document the Breach and/or Security Incident, to restore UC service(s) as directed by UC, and undertake appropriate response activities;
5. Providing status reports to UC regarding Breach and Security Incident response activities, either on a daily basis or a frequency approved by UC;
6. Coordinating all media, law enforcement, or other Breach and/or Security Incident notifications with UC in advance of such notification(s), unless expressly prohibited by law;
7. Ensuring that knowledgeable Supplier employees are available on short notice, if needed, to participate in UC and Supplier initiated meetings and/or conference calls regarding the Breach and/or Security Incident; and
8. Ensuring that knowledgeable Supplier employees and agents participate in after-action analysis, including root cause analysis and preventive action planning.

E. Breaches and Security Incidents – Corrective and Preventive Action: As a result of a Breach and/or Security Incident impacting Institutional Information and/or IT Resources, and upon UC's request, Supplier must prepare a report detailing corrective and preventive actions. The report must include:

1. A mutually agreed upon timeline for the corrective and preventive actions based on the nature of the Breach and/or Security Incident;
2. Identification and description of the root causes; and
3. Precise steps Supplier will take to address the failures in the underlying administrative, technical, and/or physical controls to mitigate damages and future cyber risk.

F. Costs: Supplier must reimburse UC for reasonable costs related to responding to Breaches impacting Institutional Information and IT Resources caused by Supplier. This includes all costs associated with notice and/or remediation of the Breach.

G. Grounds for Termination: Any Breach may be grounds for termination ofthe Agreement by UC. Agreement obligations to secure, dispose, and report continue through the resolution of the Breach and/or Security Incident.

ARTICLE 10. ILLICIT CODE WARRANTY[3]

A. Supplier represents and warrants that the Goods and/or Services do not contain Illicit Code.

B. To the extent that any Goods and/or Services have Illicit Code written into them, Supplier will be in breach of this Agreement, and no cure period will apply.

C. Should Supplier learn of the presence of Illicit Code, Supplier will promptly provide UC with written notice explaining the scope and associated risk.

D. Supplier represents and warrants that it will take commercially reasonable steps to promptly remove Illicit Code.

ARTICLE 11. BACKGROUND CHECKS

A. Before Supplier's employee, sub-supplier, or agent may access Institutional Information and/or IT Resources classified at Protection Level 3 or Protection Level 4[4], Supplier must conduct a thorough and pertinent background check. Supplier must evaluate the results prior to granting access in order to assure that there is no indication that the employee, sub-supplier, or agent presents a risk to Institutional Information and IT Resources.

B. Supplier must retain each employee's, sub-supplier's, or agent's background check documentation for a period of three (3) years following the termination of the Agreement.

[3] This provision does not relate to malware or viruses that attack the running IT Resource. These are covered under ARTICLE 9 - COORDINATING, REPORTING, AND RESPONDING TO BREACHES AND SECURITY INCIDENTS.

[4] See Exhibit 1.

Exhibit 1 – Institutional Information

This exhibit describes the Institutional Information for the benefit of both parties.

1. Protection Level Classification[5]:

Protection Levels Needed	Anticipated Record Count
☐ Protection Level 1	
☐ Protection Level 2	
☐ Protection Level 3	☐ Less than 70,000 ☐ More than 70,000
☐ Protection Level 4	☐ Less than 70,000 ☐ More than 70,000

Explanation:	

The Protection Level and anticipated record count determines the applicable cyber security insurance requirement in the Terms and Conditions.

2. Institutional Information data element descriptors:

Select all data types that apply:

A. ☐ Animal Research Data.
B. ☐ Controlled Technical Information (CTI).
C. ☐ Controlled Unclassified Information (CUI) – 800-171/NARA.
D. ☐ Defense Department: Covered Defense Information (CDI).
E. ☐ Federal Acquisition Regulations (FARS/DFAR) other than CUI.
F. ☐ European Privacy Law (EEA and UK GDPR) personal data.
G. ☐ European Privacy Law (EEA and UK GDPR) special data.
H. ☐ Health data – other identifiable medical data not covered by HIPAA. (Including but not limited to: occupational health, special accommodation, or services qualification, etc.)
I. ☐ Health Records subject to HIPAA Privacy or Security Rule (PHI).
J. ☐ Human Subject Research Data.
    1. ☐ Identified.
    2. ☐ Anonymized.
K. ☐ Intellectual property (IP), such as patents, copyright, or trade secrets.
L. ☐ ITAR/EAR-controlled data.

[5] For more information about classification see: https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html.

M. ☐ Payment card data (PCI, PCI DSS).
N. ☐ Personally identifiable information – PII.
O. ☐ Student data, whether or not subject to FERPA.
P. ☐ Other: _____
Q. ☐ Other: _____

3. Regulation or Contracts Relating to the Institutional Information:

Select all regulations or external obligations that apply to inform UC and the Supplier of obligations related to this Appendix:

Privacy (* indicates data security requirements are also present)

A. ☐ California Confidentiality of Medical Information Act (CMIA) *.
B. ☐ California Consumer Privacy Act (CCPA).
C. ☐ California Information Practices Act (IPA).
D. ☐ European Privacy Laws Regulation (EEA and UK GDPR)*.
E. ☐ Family Educational Rights and Privacy Act (FERPA) *.
F. ☐ Federal Policy for the Protection of Human Subjects ("Common Rule").
G. ☐ Genetic Information Nondiscrimination Act (GINA).
H. ☐ Gramm-Leach-Bliley Act (GLBA) (Student Financial Aid) *.
I. ☐ Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH) *.
J. ☐ Substance Abuse and Mental Health Services Administration SAMHSA (CFR 42 Part 2).
K. ☐ The Fair and Accurate Credit Transaction Act (FACTA).
L. ☐ The Fair Credit Reporting Act (FCRA).

Data Security

M. ☐ Chemical Facility Anti-Terrorism Standards (CFATS).
N. ☐ Defense Federal Acquisition Regulations (DFARS).
O. ☐ Export Administration Regulations (EAR).
P. ☐ Federal Acquisition Regulations (FARS).
Q. ☐ Federal Information Security Modernization Act (FISMA).
R. ☐ International Traffic in Arms Regulations (ITAR).
S. ☐ Payment card data (PCI, PCI DSS).
T. ☐ Toxic Substances Control Act (TSCA).
U. ☐ Other: _____
V. ☐ Other: _____

Exhibit 2
Supplier's Initial Information Security Plan

ATTACHMENT 6

Approved Timekeepers Schedule

The following rates are effective through December 31, 2027 for matters billed on an hourly basis. Only those individuals listed or otherwise referenced below and listed on a matter-specific Retention Schedule may bill time or services to any individual matter.

Please note: all timekeepers must be registered in advance in the University's CounselLink system. For instructions or assistance with this process, please contact legalbilling@ucop.edu.

Contract/Temporary/Staff Attorneys or Other Personnel:

Contract, temporary, or "staff" attorneys and other professionals are not eligible to perform work according to the above fee schedule but may be approved by a UC Monitor to work on any matter where their participation will make the retention as a whole more cost effective than would otherwise be the case (for example to facilitate diligence or discovery activities); provided, however, that: (i) Firm shall remain responsible for their oversight and work product; and (ii) any mark-up over the hourly rate at which they are being paid accurately reflects associated administrative and overhead costs, is approved in advance by the UC Monitor, and in any event does not exceed twenty percent (20%).