Procurement and Contracting Services

Request for Proposals for an Alternative Medical, Dental, and Vision Plan for Employees with Domestic Partners

ADDENDUM #2

Please mark all proposal submission Envelopes with the following information

Sealed RFP # L192221, L192222, L192223
Due on June 15, 2022, no later than 2:00 PM, MST

L192221, L192222, L192223:

- Please see the attached Information Security and Privacy Addendum.

- The University will not release any individually identifying information, such as names of insured or medical diagnosis. Please bid based on the information provided in the census and claims history information.

L192222:

- Claims history and network providers are available for the Dental PPO plan. Contact Celeste Kanzig cdkanzig@arizona.edu.

End of addendum, all else remains the same.

University of Arizona Information Security and Privacy Addendum

This Information Security and Privacy Addendum ("ISPA") is between the Arizona Board of Regents on behalf of The University of Arizona ("University") and [VENDOR] ("Vendor") and is hereby incorporated into the Agreement between the parties dated [DATE] (the "Agreement"). Vendor is providing [description of services] (the "Services"), and by doing so, add the following terms and conditions as an addendum.

1. **Definitions** Capitalized terms used but not defined in this ISPA have the same meanings as set out in the Agreement.

Cloud Software means any externally hosted technology offering which enables on-demand Network access to a shared pool of configurable computing resources.

EEA means the European Economic Area (including the United Kingdom).

Medical Records means all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers.

Network means any University network to which Vendor is provided access in connection with the performance of Services under the Agreement and/or any Vendor network that may access University Data.

Process or Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal Information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, device, or household.

Security Incident means any accidental, attempted, unlawful, or unauthorized destruction, alteration, disclosure, misuse, loss, theft, access, copying, modification, disposal, compromise, or access to University Data or any act or omission that compromises or undermines the physical, technical, or administrative safeguards put in place by Vendor in Processing University Data or otherwise performing the Services.

System means any desktop or laptop, mobile device, server and/or storage device that, (i) is involved in the performance of the Services, (ii) may be used to access a Network, or (iii) may access or store University Data.

University Data means any and all data, information, text, graphics, works, and other materials that are collected, loaded, stored, accessible, transferred through and/or accessed by Vendor or provided to Vendor by University. This includes University's Systems and Network and also includes, but is not limited to: (1) all of the deliverables, reports, or materials from the Services; (2) all University information and materials that Vendor develops or acquires prior to, or independently of, the Agreement; (3) and any Personal Information or Medical Records pertaining to University end users, students, staff, patients or any other individuals identified in materials provided to or made accessible to Vendor by University. University Data is Confidential Information.

2. **Restrictions on University Data Use**

a. Vendor represents and warrants that it will only collect, access, use, maintain, and Process University Data for the sole and exclusive purpose of providing the Services in the Agreement, and may not retain, collect, use or disclose the University Data for any purpose other than performing the Services. Vendor may not share or sell the University Data for any reason or disclose the University Data to any third party except to provide the Services specified in the Agreement.

b. Upon termination or expiration of the Agreement or upon written request from University, whichever comes first, Vendor will, and will ensure that its Representatives (as defined below), immediately cease all use of and return to University or, at the direction of University, destroy all such University Data provided under this Agreement. If University elects for destruction, Vendor must certify to University that such University Data has been destroyed. If Vendor is required by law to retain any University Data, Vendor must notify University of such requirement and will maintain the confidentiality of such University Data and may not use University Data for any purpose other than as required by law.

c. Vendor will limit access to University Data to its employees, contractors, subcontractors, and/or agents ("Representatives") whose access is necessary to carry out the Services and will ensure those Representatives to keep all University Data confidential. Vendor will inform all Representatives of the confidential nature of University Data and all Representatives will be bound by confidentiality agreements with similar or greater confidentiality and security obligations as Vendor provides to University in the Agreement. Vendor agrees to be legally and financially liable for any breach of this ISPA, or unauthorized disclosure or misuse of University Data by its Representatives. The access rights of any Representatives will be removed immediately by Vendor upon termination or adjusted when such access is no longer necessary. Unless expressly consented to by University, Vendor will host and only allow access to University Data in the United States.

d. If Vendor and its Representatives will have access to University Data, Systems, or Networks, Vendor must ensure that its Representatives have undergone annual privacy and security training and adhere to Vendor's policies and procedures that relate to privacy and security.

e. If Vendor is contacted by a third party with a request, inquiry, or complaint regarding University Data, Vendor will promptly (a) and in any event within two (2) calendar days,

provide University with written notice of such request, inquiry or complaint to security@arizona.edu; and (b) provide University all reasonable cooperation, assistance, information and access to such data in its possession or control as is necessary for University to respond to such request, inquiry or complaint. Vendor will not respond to such request, inquiry or complaint unless so instructed in writing by University.

3. **Written Information Security Program**

a. At all times during the term of the Agreement, Vendor will implement and maintain a written information security program ("WISP"), which must include appropriate administrative, technical, physical, and operational safeguards to maintain the security, privacy, availability, integrity, and confidentiality of University Data in use, in motion, and at rest.

b. Vendor will implement and maintain a formalized risk governance plan, policy, and a continuous risk assessment process demonstrating Vendor's ability to identify, quantify, prioritize, and mitigate risks. If requested by University, Vendor will (and/or cause subcontractors to) certify its compliance with the requirements of this ISPA and provide written responses to any reasonable questions submitted to Vendor by University. Vendor agrees to conduct and provide to University a Data Protection Impact Assessment ("DPIA") or an independent audit report, if reasonably requested by University.

4. **Data Privacy and Security**

a. Vendor agrees to implement and maintain administrative, technical, physical, and operational safeguards in accordance with industry best practices at a level sufficient to secure University Data.

b. Vendor agrees to maintain the following enterprise controls for any Networks or Systems that host, Process, or provide access to University Data:

i. Asset and Information Management. Vendor will maintain and enforce policies and controls that include, without limitation, asset inventory/management, encryption (in transit and at rest), storage of data on portable hardware, and third-party access to and use of University Data.

ii. Human Resources Security. Vendor will maintain and enforce a policy that addresses human resources security for all Representatives accessing University Data. Vendor will conduct background checks and not utilize any individual to fulfill the obligations of this Agreement if such individual has been convicted of any crime involving dishonesty or false statement including, but not limited to fraud and theft, or otherwise convicted of any offense for which incarceration for a minimum of one (1) year is an authorized penalty. Any such individual may not be a "Representative" under this Agreement

iii. Physical Security. All facilities used by or on behalf of Vendor to store and process University Data will implement and maintain administrative, physical, technical, and procedural safeguards in accordance with industry best practices at a level sufficient to secure University Data from a Security Incident. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event, less than reasonable in view of the type and nature of the data involved.

iv. Data and System Access Controls. Vendor will maintain and enforce policies and controls that include, without limitation, role-based permissions for access to University Data (using a principle of minimization), restrictions on copying or removing data from an authorized network or system, strong password protocols (i.e., complexity requirements, mandatory changes, restrictions on sharing, etc.), and multi-factor authentication or equivalent protections for any remote access to Vendor's network or systems. Vendor will trace approved access to ensure proper usage and accountability, and the Vendor will make such information available to the University for review, upon the University's request and not later than five (5) business days after the request is made in writing.

v. Availability Control. Vendor will take industry-standard steps to ensure that University Data is available when requested by University. Additionally, Vendor must take steps to protect against accidental destruction or loss of University Data, including, without limitation, anti-virus software; firewalls; network segmentation; user of content filter/proxies; interruption-free power supply; threat detection and prevention; regular generation of and testing of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; business continuity and emergency plans; and air-conditioned server rooms.

vi. Network Security. Vendor will carry out updates and patch management for all systems and devices in a timely manner, applying security patches within five (5) business days or less based on reported criticality. Updates and patch management must be deployed using an auditable process that can be reviewed by the University upon the University's request and not later than five (5) business days after the request is made in writing. An initial report of patch status must be provided to the University prior to the effective date of the Agreement. Vendor will maintain documented operating procedures and technological controls to ensure the effective management, operation, and security, of Vendor's Network, including, without limitation, an up-to-date Network diagram, wireless encryption protocols, and adequate remote access protocols.

vii. Logging and Monitoring. Vendor will comply with relevant security best practices for the monitoring and logging of its Networks, applications, and Systems. Logs will be kept for the duration of the Agreement or Vendor's record retention policy, whichever is longer.

viii. Change Management and Web Applications. Vendor will use secure development and coding standards in accordance with industry standards. Vendor's web applications must meet OWASP Application Security Verification Standards (ASVS). Vendor will perform adequate testing prior to releasing updates, modifications, or new functionality to software.

5. **Representations and Warranties**

a. Vendor represents and warrants that: (i) it will comply

with the requirements under applicable privacy and data security laws (including, if applicable, the General Data Protection Regulation (GDPR), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999), the Children's Online Privacy Protection Act (COPPA), and/or Payment Card Industry Data Security Standard (PCI DSS)), and applicable state privacy and security laws; (ii) it will comply with the requirements of this ISPA, and (iii) it will perform the Services in accordance with industry standards and in a professional and workmanlike manner. If the Agreement requires or permits Vendor to access, receive, or release any student records, then, for purposes of this Agreement only, University designates Vendor as a "school official" for University under FERPA, as that term is used in FERPA and its implementing regulations.

b. If Vendor is provided access to Medical Records, but the applicable information is not subject to HIPAA, Vendor represents and warrants that it will (i) comply with 16 C.F.R, Part 318 and (ii) only use or disclose Medical Records as permitted or required under the Agreement, or as required by law. At all times during the course of the Agreement, Vendor will make any Medical Records available to University for access, portability, modification, or deletion.

c. Vendor represents and warrants that all responses to any security assessment by University are accurate and truthfully represents the security practices of Vendor. Vendor agrees that, at the request of University, it will provide sufficient evidence of its compliance with obligations set forth in this ISPA.

6. **Data Security Incident**

a. Vendor will maintain, update and document an Incident Response Plan ("IRP"), and will manage, document, review, investigate and resolve all Security Incidents in accordance with the IRP.

b. Vendor agrees to notify University of a Security Incident at security@arizona.edu as soon as reasonably practicable and without undue delay. Such notice must include (i) a description of the incident, including the type of incident (e.g., theft, loss, improper disclosure, unauthorized access), location of the incident (e.g., laptop, desktop, paper), how the incident occurred, the date the incident occurred, and the date the incident was discovered; (ii) a description of the type of University Data involved (e.g., user data, intellectual property, etc.); (iii) a description of the potentially impacted individuals; (iv) a description of the actions taken in response to the Security Incident (e.g., additional safeguards, mitigation, sanctions, policies, and procedures); and (v) all other information reasonably requested by University or necessary to provide notice to individuals and/or regulators, including a forensic report summarizing the findings of a forensic investigation. University acknowledges that certain information may not be immediately available and can be provided on a rolling basis as it is discovered (within 72 hours of discovery).

c. In facilitating the investigation and remediation of a Security Incident, Vendor will cooperate fully with University. Vendor may not inform any third party of any Security Incident without first obtaining the University's written consent, except as may be required by law. Vendor agrees to reimburse University for reasonable costs and expenses incurred (including legal fees) in responding to, remediating, and/or mitigating damages caused by a Security Incident or in following up on a complaint by an individual or a regulator. Vendor will take all necessary and appropriate corrective actions, including as may be reasonably instructed by University, to remedy or mitigate any Security Incident.

7. **Audit and Testing**

a. Vendor will complete one of the following audits at least annually and immediately after any actual or reasonably suspected Security Incident: SOC 2 Type II, SOC for Cybersecurity, or an accepted Higher Education Cloud Vendor Assessment Tool (https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit). Evidence must be provided to the University prior to this Agreement and at least annually thereafter.

b. Prior to this Agreement, and at regular intervals of no less than annually and whenever a change is made which may impact the confidentiality, integrity, or availability of University Data, and in accordance with industry standards and best practices, Vendor will, at its expense, perform scans for unauthorized applications, services, code and system vulnerabilities on the Networks and Systems used to perform Services related to this Agreement ("Security Tests"). An initial report must be provided to the University prior to this Agreement. Vendor will provide the University the reports or other documentation resulting from the audits, certifications, scans and tests within five (5) business days of Vendor's generation or receipt of such results. If any critical finding is identified, Vendor agrees to notify the University and remediate the critical finding within thirty (30) days. Any critical finding not remediated within thirty (30) days must be reported to University at security@arizona.edu. All other findings must be remediated within ninety (90) days. At University's request, Vendor will promptly provide written attestation that required Security Tests, independent audits, and/or a DPIA have been conducted either by a qualified Representative or by a third party in the prior twelve (12) months. The University may require the Vendor to perform additional audits and tests, the results of which will be provided to the University within five (5) business days of the Vendor's receipt of such results.

c. Vendor agrees to take reasonable steps to assist University in maintaining the accuracy of such University Data under the control of Vendor, including synchronizing relevant Systems, databases, or applications, as deemed necessary by University. The University reserves the right to, at a minimum, an annual, review of: Vendor's access reports related to access to University Data; Vendor's patch management process, schedules, and logs; findings of vulnerability scans and/or penetration tests of Vendor Systems; and Vendor development standards and processes.

8. **International Transfers**

a. If University provides its written consent for Vendor to transfer Personal Information from EEA countries to countries outside the EEA, the terms set out in the EU

Standard Contractual Clauses will apply. The parties will work in good faith to populate appendices 1 and 2 of the EU Standard Contractual Clauses and attach an executed version to this ISPA. Vendor agrees to comply with all obligations imposed on a "data importer" set out in such EU Standard Contractual Clauses. For countries located within the Asia Pacific region, Vendor must obtain University prior written consent where Personal Information will be transmitted by the Vendor outside the country from which it was originally collected.

9. **Insurance**

a. Without limiting any liabilities or any other obligation of Vendor, Vendor will purchase and maintain (and cause its subcontractors to purchase and maintain), until all of their obligations under the ISPA have been discharged or satisfied, insurance against claims that may arise from or in connection with the Services, as described here: https://risk.arizona.edu/sites/default/files/InsuranceRequirements5_12_2020.pdf

b. Vendor's Technology Professional Liability Errors & Omissions policy must include Cyber Risk coverage and Computer Security and Privacy Liability coverage with a limit of no less than $2,000,000 per occurrence and $4,000,000 in the aggregate. This policy will provide for both first- and third-party costs, and name University as an additional insured with respect to the provision of Services. This policy will include a waiver of subrogation against University.

c. The required insurance coverage set forth above will not be construed as a limitation or waiver of any potential liability or obligation of Vendor in the Agreement. Failure to maintain the insurance coverage identified in this Section will constitute a material breach.

10. **Appendices**

a. If Vendor is a Cloud Software provider, then the Cloud Software Appendix will apply.

b. If Vendor is processing credit or debit card transactions on behalf of University, the PCI Appendix will apply.

c. If Vendor is collecting, accessing, acquiring, or otherwise Processing Protected Health Information (as defined in the Health Insurance Portability and Accountability Act of 1996), then the PHI Appendix/Business Associate Agreement will apply.

11. **Miscellaneous**

a. Vendor's obligations under this ISPA will survive the termination or expiration of the ISPA and will apply so long as Vendor may access or be in possession of University Data, Network, or Systems. Any requirements imposed on Vendor in this ISPA shall apply to any of Vendor's subcontractors. Following the termination of the Agreement for any reason, Vendor agrees to provide transition services for the benefit of University, including a month-to-month extension (not to exceed ninety (90) days) for the continued provision of its Services and reasonable assistance with the transfer of University Data. The parties agree to take such reasonable actions as are necessary to amend this ISPA from time to time as is necessary for the parties to comply with applicable privacy laws. In the event of inconsistency between the Agreement and the ISPA, the ISPA will govern.

The parties have executed and delivered this ISPA effective as of [Date].

The University of Arizona	**Vendor**
By:_____	By:_____
Name:_____	Name:_____
Date:_____	Date:_____

Cloud Software Appendix

In addition to the terms in the ISPA, the following terms will apply if the Services provided under this Agreement are provided to University as Cloud Software.

1. **Vendor Obligations.** In addition to any other obligations of Vendor, Vendor must:
    a) Provide the Services on a continuous basis and warrants that the Services will be fully available 99.9% of each month, except for scheduled maintenance for which written notice has been provided to University at least thirty (30) calendar days in advance.
    b) Provide unlimited telephone support twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year ("24/7/365").
    c) Provide online access to technical support bulletins and other user support information and forums 24/7/365;
    d) Conduct quarterly support updates and reviews involving technical teams from both Parties to discuss Cloud Software support issues.
    e) Provide semi-annual support usage, incident reports and Vendor's compliance with any service levels identified in a service level agreement.
    f) Respond with support to Priority One Issues (as defined below) within one (1) hour of University's call for assistance to Vendor and initiate work on such issues within one (1) hour thereafter, regardless of time of day or day of week. Priority One Issues include issues involving substantial failure of the Cloud Software, which, in University's sole judgment, are critical to its operations. Vendor will initiate work on all other support issues, within four (4) hours from receipt of an electronic or telephonic service request.
    g) In the event two or more Priority One Issues occur in any thirty (30) day period during the term of the Agreement, Vendor will promptly investigate the root causes of such support issues and will provide to University an analysis of such root causes and a proposed corrective action plan for University's review, comment and approval (the "Corrective Action Plan"). The Corrective Action Plan must include, at a minimum: (i) a commitment by Vendor to University to devote the appropriate time, skilled personnel, systems support and equipment, and/or resources to remedy, and prevent any further occurrences of Priority One Issues; (ii) a strategy for developing any programming/software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of such issues; and (iii) time frames for implementation of the Corrective Action Plan. There will be no additional charge (other than those fees set forth in this Agreement) for Vendor's implementation of such Corrective Action Plan in the time frames and manner set forth in the Corrective Action Plan.

2. **Scheduled Maintenance of Cloud Software.** Scheduled maintenance, updates, enhancements or modifications relative to the Services and/or other elements or components of the Services will be in accordance with Vendor's maintenance schedule and will not in any way diminish the benefits, comprehensiveness, features or functionality of the Services, as defined under the Agreement. Vendor may, however, push updates and fixes at any time to University that Vendor determines will not affect University's ability to access the Services. Unless otherwise agreed in writing, non-peak hours are from Friday night at 11:00 p.m. MST through Saturday morning at 8:00 a.m. MST, and Saturday night at 11:00 p.m. MST through Sunday morning at 8:00 a.m. MST.

3. **Unscheduled Maintenance of Cloud Software**. If the Services provided under this Agreement are provided to University as Cloud Software, Vendor will provide University with at least seventy-two (72) hours prior notice of Vendor's implementation of all unscheduled maintenance, updates, enhancements, modifications and/or other circumstances which will result in an outage or an inability of University to access the Services. In the event emergency maintenance of the Services is required, Vendor will provide University with as much advance notice as possible of the impending emergency maintenance and will disclose to University, in writing, the cause or issue necessitating the emergency maintenance as soon as possible and no later than seventy-two (72) hours after the initiation of the emergency maintenance.

4. **Critical Services Not to be Abandoned.** Vendor acknowledges that the Cloud Software provided under this Agreement are critical services for University. Accordingly, notwithstanding any other provisions under the Agreement to the contrary, the Parties agree that Vendor may not "**Abandon"** such critical Services. For purposes of an Agreement, "Abandon" means Vendor's actual, willful non-performance of any material aspect of the Services in

breach of the Agreement which results in a material adverse effect on (i) critical aspects of University's internal operations, regulatory or other reporting requirements; or (ii) a Service that is provided to or in support of University's students and faculty. Abandonment will not be deemed to have occurred if non-performance is caused by circumstances outside of Vendor's control or if a Service is properly terminated in accordance with Vendor's rights under the Agreement. In addition, support provided under this Agreement will not be withheld due to any unrelated dispute arising under this Agreement, another agreement between the Parties, or any other unrelated dispute between the Parties.

5. **Public Cloud.** Vendor will not create a public cloud account on behalf of University without prior written approval by University's IT Security team.

6. **Cloud Management.** Vendor is responsible for continuous vulnerability management of hardware and software, including, without limitation, scanning and issue remediation. Vendor is responsible for all disruptions and damage caused to any University Data while it is hosted in Cloud Software.

7. **Hosting Facilities.** University may select or restrict where University Data will be stored and where University Data can be Processed, and the Vendor will store and/or Process it there in accordance with the service terms. If a data location selection is not covered by the service terms (or a data location selection is not made by University with respect to any University Data), the Vendor will default to a United States-based data location in the selection of University storage or processing facilities. Unless stated otherwise in this Agreement, this requirement does not apply to indirect or "overhead" services, redundant back-up services or services that are incidental to the performance of this Agreement. This provision applies to work performed by subcontractors at all tiers and to all University Data.

PCI Appendix

In addition to the terms in the ISPA, the following terms will apply if the Services provided under this Agreement involve processing credit and/or debit card transactions.

1. **Payment Card Industry Data Security Standard.** For e-commerce business and/or payment card transactions, Vendor will comply with the requirements and terms of the rules of all applicable payment card industry associations or organizations, as amended from time to time (PCI Security Standards), and be solely responsible for security and maintaining confidentiality of payment card transactions processed by means of electronic commerce up to the point of receipt of such transactions by a qualified financial institution.

2. Vendor will, at all times during the term of this Agreement, be in compliance with the then current standard for Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS) for software, and PIN Transaction Security (PCI PTS) for hardware. Vendor will provide attestation of compliance to University annually by delivering to University current copies of the following: (i) Vendor's "Attestation of Compliance for Onsite Assessments – Service Providers;" (ii) an attestation that all University locations are being processed and secured in the same manner as those in Vendor's "PCI Report on Compliance;" and (iii) a copy of Vendor's PCI Report on Compliance cover letter. Vendor will notify University immediately if Vendor becomes non-compliant, and of the occurrence of any security incidents (including information disclosure incidents, network intrusions, successful virus attacks, unauthorized access or modifications, and threats and vulnerabilities) in accordance with the ISPA.

3. Vendor's services must include the following:

   (a) Vendor maintains its own network operating on its own dedicated infrastructure. Vendor's network includes a firewall that: (i) includes access control rules that separate Vendor's PCI network from University, and (ii) restricts any communication between Vendor's network devices and University Systems.

   (b) Vendor treats the University Network as an untrusted network and no unencrypted cardholder data traverses or otherwise is stored on University Network, and University has no ability to decrypt cardholder data.

   (c) All devices must be SRED (secure reading and exchange of data), EMV (Europay, MasterCard and VISA) and PTS POI compliant.

PHI APPENDIX
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("**BAA**") is by and between the Arizona Board of Regents, acting on behalf of the University of Arizona (the "**Covered Entity**"), and **Vendor** (the "**Business Associate**") and is part of the Underlying Agreement between the Parties. Covered Entity and Business Associate are sometimes referred to herein individually as a "Party" and collectively as the "Parties."

Covered Entity and Business Associate have entered into an underlying agreement ("**Underlying Agreement**"), pursuant to which Business Associate performs functions or activities on behalf of, or provides certain services (collectively "**Services**") as an independent contractor to Covered Entity, and in connection with the Services, Business Associate may have access to, or create, receive, maintain, use, or disclose Protected Health Information ("**PHI"**). The Services to be provided by Business Associate are identified in the Underlying Agreement.

Both Parties are required to comply with the Health Information Technology Economic and Clinical Health ("**HITECH**") Act, the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") and applicable regulations issued thereunder, including, but not limited to, the Privacy, Security, Breach Notification and Enforcement Rules (45 C.F.R. Parts 160, 162 and 164), as may be amended from time to time (collectively, the "**HIPAA Rules**"). This BAA sets forth the terms and conditions pursuant to which any Protected Health Information, including electronic Protected Health Information, will be handled by Business Associate and certain third parties during the term of the Underlying Agreement and after its termination. The Parties agree as follows:

1. DEFINITIONS

All capitalized terms used but not otherwise defined in this BAA will have the meaning set forth in HIPAA/HITECH and the HIPAA Rules as in effect or as amended or supplemented from time to time. Without limiting the generality of the foregoing, the following terms, to the extent used in this Agreement, will have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Use and Workforce.

2. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION BY BUSINESS ASSOCIATE

(a) Performance of Services. Pursuant to the Underlying Agreement, Business Associate provides Services for Covered Entity that may involve the use and disclosure of Protected Health Information. Except as otherwise specified herein, Business Associate may use Protected Health Information to the extent necessary to perform its obligations under the Agreement, provided that (i) such use complies with and does not violate HITECH, HIPAA or the HIPAA Rules or (ii) such use is expressly permitted by this BAA. In conducting activities under the Underlying Agreement that involve the use or disclosure of Protected Health Information, Business Associate will limit the use or disclosure of Protected Health Information to the minimum amount of information necessary to accomplish the intended purpose of the use or disclosure. To the extent Business Associate is to carry out one or more of Covered Entities' obligations under HIPAA or HITECH, Business Associate agrees to comply with the legal requirements that apply to Covered Entities in the performance of such obligation(s).

(b) Proper Management and Administration. Except as otherwise expressly limited in this BAA or the Underlying Agreement, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that any disclosure of information received in such capacity will be made only if: (i) Required by law; or (ii) Business Associate obtains written reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any breaches of the confidentiality of the PHI.

(c) Data Aggregation. In addition to using the Protected Health Information to perform the Services set forth in Section 2(a) of this BAA, Business Associate may use Protected Health Information for Data Aggregation purposes for the Health Care Operations of Covered Entity only, and only if expressly authorized under the Underlying Agreement. Business Associate may not de-identify Protected Health Information received from or created on behalf of Covered Entity unless such de-identification is expressly permitted by the Underlying Agreement or this BAA or unless Business Associate obtains Covered Entity's prior written consent to such de-identification.

(d) Prohibition on Sale of Protected Health Information. Business Associate agrees to comply with the prohibition of sale of PHI without authorization unless an exception under 45 C.F.R. §164.508 applies. This prohibition does not apply to the disclosure

of PHI in connection with the Services performed under this Agreement where the only remuneration provided is for the performance of such Services, or to any other activity excluded from the definition of "Sale" under 45 C.F.R. § 164.502(a)(5(ii).

(e) Marketing and Fundraising**.** Business Associate will not use or disclose PHI for marketing or fundraising purposes, except with the prior written authorization of the Covered Entity and consistent with the requirements of 45 C.F.R. §§ 164.514(f) and 164.508(a)(3).

3. OBLIGATIONS AND RESPONSIBLITIES OF BUSINESS ASSOCIATE WITH RESPECT TO PROTECTED HEALTH INFORMATION

Business Associate hereby agrees to do the following:

(a) Use and Disclosure of PHI. Use or disclose the Protected Health Information only as permitted or required by the Underlying Agreement or this BAA or as otherwise Required by Law. Business Associate will not, without the prior written consent of Covered Entity, disclose any Protected Health Information on the basis that such disclosure is Required by Law without first notifying Covered Entity so that Covered Entity will have an opportunity to object to the disclosure and to seek appropriate relief unless immediate disclosure is Required by Law. Business Associate will require reasonable assurances from third parties receiving Protected Health Information in accordance with Section 2(b) hereof that such third parties will provide Covered Entity with similar notice and opportunity to object before disclosing Protected Health Information on the basis that such disclosure is Required by Law. Business Associate may disclose Protected Health Information for the purposes authorized by this Agreement only (i) to members of its Workforce, (ii) to its Subcontractors (as defined below) and agents in accordance with Section 3(d), (iii) as directed by Covered Entity in accordance with this BAA, or (iv) as otherwise permitted by the terms of this BAA including, but not limited to, Section 2(b) above. Any other use or disclosure not permitted or required by this Agreement is prohibited.

(b) Reports in Writing. Business Associate must report to the designated Privacy Officer of Covered Entity, in writing, any Breach or Security Incident of which Business Associate becomes aware as soon as possible, and at least within three (3) days of Business Associate's discovery of any of the foregoing (for purposes hereof, "discovery" will have the meaning ascribed to it in 45 CFR § 164.404(a)(2)). In the event of a Breach or Security Incident that arises from the actions or omissions of Business Associate or its employees, Subcontractors, agents, representatives or other members of its Workforce, and that requires notification of government agencies or patients, Business Associate will cooperate fully with Covered Entity in Covered Entity's efforts to carry out the notification and mitigation requirements and will indemnify and reimburse Covered Entity for all of Covered Entity's costs of complying with and carrying out such requirements.

(c) Mitigation. Mitigate, to the greatest extent practicable, any harmful effects from any Breach or any Security Incident of which Business Associate becomes aware.

(d) Safeguards. Comply with the Security Rule to maintain the security of, and prevent any unauthorized use or disclosure of, electronic Protected Health Information. Business Associate will maintain and implement a comprehensive information privacy and security program that complies with HITECH, HIPAA, and the regulations and guidance issued thereunder by the United States Department of Health and Human Services ("**HHS**"). Without limitation, this includes administrative, technical and physical safeguards that are appropriate to the size and complexity of Business Associate's operations and the nature and scope of its activities involving Protected Health Information. Business Associate will comply with the HHS guidance to render unsecured PHI unusable, unreadable, or indecipherable to unauthorized individuals, with respect to ePHI in motion and at rest, and destruction of PHI. In addition, in the event that the Underlying Agreement contains specific requirements regarding information and data security, Business Associate will comply with all such provisions of the Agreement.

(e) Subcontractors. Require any person(s) to whom Business Associate delegates a function, activity or service under the Agreement (other than members of Business Associate's Workforce) or who create, receive, maintain or transmit Protected Health Information on behalf of or for Business Associate ("**Subcontractors**") and agents that receive or use, or have access to, Protected Health Information to enter into a written agreement that, (i) complies with HITECH and HIPAA, (ii) includes the same restrictions, conditions, obligations and requirements concerning Protected Health Information that apply to Business Associate pursuant to this BAA; and (iii) provides that all assignees or subcontractors of Business Associate's Subcontractor will enter into written agreements satisfying the requirements of clauses (i) through (iii) above. Before allowing any subcontractor or agent that is not organized under the laws of any state within the United States ("**Foreign Subcontractor**") to use or disclose, or have access to, Protected Health Information, Business Associate will obtain the prior written consent of Covered Entity to the use of such Foreign Subcontractor, which consent may be withheld in Covered Entity's sole discretion.

(f) Accounting of Disclosures of PHI. Business Associate must:

(i) Maintain and make available the information required to enable Covered Entity to respond to an individual's request for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528; and

(ii) Within five (5) days of receiving a written request from Covered Entity, provide to Covered Entity such information as is requested by Covered Entity to permit Covered Entity to respond to a request by an individual for an accounting of the disclosures of the individual's Protected Health Information in accordance with 45 C.F.R. § 164.528.

(iii) In the event that an individual requests an accounting of disclosures directly from Business Associate or its agents or Subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request; Covered Entity will be responsible for preparing and delivering to the individual any such accounting requested.

(g) Availability of Records for Review by HHS and Covered Entity.

(i) Make available all records, books, agreements, policies and procedures relating to the use or disclosure of Protected Health Information to the Secretary of the U.S. Department of Health and Human Services (or any officer or employee of HHS to whom the Secretary of HHS has delegated such authority) for purposes of determining Covered Entity's compliance with the Privacy Rule and Security Rule, subject to attorney-client and other applicable legal privileges. Business Associate will immediately notify Covered Entity upon receipt by Business Associate of any complaint or request for access by the Secretary of HHS and will provide Covered Entity with a copy thereof as well as a copy of all materials disclosed pursuant thereto.

(ii) Upon reasonable prior written notice, make available during normal business hours at Business Associate's offices all policies, procedures and related materials pertaining to the use or disclosure of, and security of, Protected Health Information to Covered Entity for purposes of enabling Covered Entity to determine Business Associate's compliance with the terms of this Agreement.

4. RESPONSIBILITIES OF BUSINESS ASSOCIATE WITH RESPECT TO HANDLING OF DESIGNATED RECORD SET

In the event that the Protected Health Information received by Business Associate pursuant to the Underlying Agreement constitutes a Designated Record Set, Business Associate hereby agrees to do the following:

(a) Access. At the request of Covered Entity, provide access to the Protected Health Information to Covered Entity for inspection or copying, to enable Covered Entity to fulfill its obligations under 45 C.F.R. § 164.524. In the event that an individual requests access to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request; Covered Entity will be responsible for delivering to the individual the information he or she has requested.

(b) Amendment. At the request of Covered Entity, make any amendment(s) to the Protected Health Information that Covered Entity directs pursuant to 45 C.F.R. § 164.526. In the event that any individual requests an amendment of Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of such request; Covered Entity will then direct Business Associate to amend its Protected Health Information, as may be appropriate based on the individual's request.

5. REPRESENTATIONS AND WARRANTIES OF BUSINESS ASSOCIATE

Business Associate represents and warrants to Covered Entity that all of its employees, agents, representatives, Subcontractors and members of its Workforce, whose services may be used to fulfill obligations under the Underlying Agreement or this BAA are or will be appropriately informed of their obligations and responsibilities regarding Protected Health Information hereunder.

6. OBLIGATIONS OF COVERED ENTITY

(a) Changes in Permission. Covered Entity will provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI provided to it by the Covered Entity, if such changes affect Business Associate's permitted or required uses and disclosures.

(b) Notification of Restrictions. Covered Entity will notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity or Business Associate has agreed to in accordance with 45 C.F.R. § 164.522.

(c) Requests to Use or Disclose PHI. Covered Entity will not request that Business Associate use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by the Business Associate or the Covered Entity.

7. TERM AND TERMINATION

(a) Term. This Agreement will become effective on the Underlying Agreement Effective Date and will continue in effect until termination or expiration of the Services Agreement, subject to the survival provisions of Section 9(a), unless terminated as provided in this Section 7.

(b) Termination by Covered Entity. As provided under 45 C.F.R. § 164.504(e)(2)(iii), Covered Entity may immediately terminate this Agreement and the Services Agreement if Covered Entity knows of a pattern of activity or practice of Business Associate that constitutes a material breach or violation of Business Associate's obligations under the provisions of this Agreement. Alternatively, if Covered Entity has determined that Business Associate has violated a material term of this Agreement and Covered Entity elects not to immediately terminate the Services Agreement and this Agreement, then Covered Entity will: (i) provide Business Associate written notice of the existence of an alleged material breach; and (ii) afford Business Associate an opportunity to cure the alleged material breach within five (5) days. In the event that Business Associate does not cure the breach within five (5) days, Covered Entity may terminate, the Services Agreement or this Agreement, if feasible (as determined by Covered Entity), or if termination is not feasible, report the problem to the Secretary of HHS.

(c) Effect of Termination. Upon termination of the Services Agreement and this Agreement pursuant to this Section 7, Business Associate must return to Covered Entity, or if agreed to by Covered Entity, destroy all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate and its agents and Subcontractors still maintain in any form. If such return or destruction is not feasible, then Business Associate will so notify Covered Entity in writing, and will (a) extend any and all protections, obligations, limitations and restrictions contained in this BAA to Protected Health Information retained by Business Associate, its agents and its Subcontractors after the termination of the Services Agreement and this Agreement, (b) limit any further uses or disclosures to those purposes that make the return or destruction of the Protected Health Information infeasible and (c) at such time as return or destruction of such retained Protected Health Information becomes feasible, return or, if agreed to by Covered Entity, destroy such Protected Health Information.

8. INDEMNIFICATION

Business Associate agrees to indemnify and hold harmless Covered Entity and its officers, agents and employees (collectively, Covered Entity's "**Indemnitees**") against all actual and direct losses, liabilities, damages, claims, costs or expenses (including Covered Entity's reasonable attorney's fees in defending itself against third party claims) they may suffer as the result of third party claims, demands, actions, investigations, settlements or judgments against them arising from or in connection with any breach of this Agreement or of any representation or warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under the Privacy Rule and Security Rule, by Business Associate or its employees, directors, officers, Subcontractors, agents or other members of its Workforce. Business Associate's obligation to indemnify Covered Entity and its Indemnitees will survive the expiration or termination of this BAA for any reason.

9. **MISCELLANEOUS**

(a) Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 3 and 7 - 9, solely with respect to Protected Health Information Business Associate retains in accordance with Section 7(c) because it is not feasible to return or destroy such Protected Health Information, will survive termination of this Agreement indefinitely. In addition, Section 4 will survive termination of this Agreement, provided that Covered Entity determines that the Protected Health Information being retained pursuant to Section 7(c) herein constitutes a Designated Record Set.

(b) Limitation of Liability. To the extent that the Agreement contains a provision that limits Business Associate's liability under the Underlying Agreement, Business Associate's obligations under this BAA, including but not limited to Business Associate's indemnification obligations under Sections 3(b) and 8 hereof, will be excluded from such limitation of liability.

(c) Entire Agreement; Amendments; Waiver. This BAA constitutes the entire agreement between the Parties pertaining to the subject matter hereof and supersedes any previous agreements between the Parties relating to the same subject matter. This BAA may not be modified, nor will any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event cannot be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

(d) No Third-Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor will anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

(e) Notices. Any notices to be given under this BAA to a Party will be made via U.S. Mail or express courier to such Party's address set forth below, or via facsimile to the facsimile telephone numbers listed below.

Covered Entity Contact:

As stated in the Underlying Agreement.

With a copy to:
HIPAA Privacy Officer
The University of Arizona
PO Box 210409
Tucson, AZ 85721
Fax: (520) 621-3355

Business Associate Contact:

As stated in the Underlying Agreement.

Each Party may change its address and that of its representative for notice by giving notice thereof in the manner provided above in this Section 9(e).

(f) Applicability. If the provision of Services involves Business Associate's receipt, maintenance or transmission of University Data that contains PHI, the Parties agree that this BAA shall become an integral part of the Underlying Agreement and shall apply to Business Associate's receipt, maintenance or transmission of PHI from, or on behalf of the Covered Entity.

(g) Interpretation; Inconsistences between Agreement and BAA; Section Headings. The provisions of this BAA will prevail over any provisions in the Underlying Agreement that may conflict or appear inconsistent with any provisions in this BAA. The Parties agree that any ambiguity in this BAA will be resolved in favor of a meaning that complies and is consistent with the Privacy Regulation and Security Regulation. The section headings used in this BAA are for reference and convenience only and have no legal or contractual effect.

(h) Governing Law. This BAA will be governed by and construed in accordance with the laws of the State of Arizona, without application of principles of conflicts of laws. The Parties hereto agree that any dispute arising under this contract will be resolved in the Arizona State courts of Pima County, Arizona or in the Federal District Court for the District of Arizona sitting in Tucson, Arizona, and the Parties hereby submit themselves to the personal jurisdiction of said courts.

(i) Amendment to Comply with Law. The Parties agree to take such action as is necessary to implement the standards and requirements of HITECH and regulations thereunder, HIPAA, the Privacy Regulation, the Security Regulation, and other applicable laws relating to the security or confidentiality of Protected Health Information. The Parties further agree to take such action as is necessary to amend this BAA from time to time as is necessary for compliance with the requirements of HITECH, HIPAA, the HIPAA Rules or other applicable laws.

(j) State Law. Nothing in this BAA will be construed to require or permit Business Associate to use or disclose Protected Health Information without written authorization from an individual who is a subject of the Protected Health Information, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure.

(k) Injunctions. Covered Entity and Business Associate agree that any violation of the provisions of this BAA will cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law, in equity, or under this BAA, in the event of any violation of any of the provisions of this BAA, or any explicit threat thereof, Covered Entity will be entitled to an injunction or other decree of specific performance with respect to such violation(s) or explicit threat thereof.

(l) Agency. The Parties agree and acknowledge that Business Associate is not an "agent" of Covered Entity as that term is defined in the federal common law.

The rest of this page left blank intentionally.

IN WITNESS WHEREOF, each of the undersigned has caused this BAA to be duly executed in its name and on its behalf as of the Effective Date

COVERED ENTITY: The University of Arizona	**BUSINESS ASSOCIATE**
Signature of Authorized Representative	Signature of Authorized Representative
Printed Name:	**Printed Name:**
Title:	**Title:**
Date:	**Date:**

Reviewed by: THE UNIVERSITY OF ARIZONA HIPAA PRIVACY OFFICER

Signature of Acknowledgement

Printed Name: **John F Howard**

Date