



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 RESPONSIBILITIES 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 can not 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; Inconsistencies 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