# BUSINESS ASSOCIATE AGREEMENT BETWEEN

**<insert company name> AND AUBURN UNIVERSITY**

This Agreement as made and entered into this \_\_\_\_\_\_\_\_\_\_\_\_ of \_\_\_\_\_\_\_\_\_\_\_\_\_\_, by and between the Auburn University on behalf of the Auburn University ˂insert AU covered entity name˃, hereinafter collectively designated as "Covered Entity", and <insert company name>, hereinafter designated as "Business Associate".

**RECITALS**

a. Auburn University is a Hybrid Entity with designated units that are covered entities as defined by HIPAA. ˂insert AU covered entity name˃ is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Covered Entity must comply with the Administrative Simplification Provisions of HIPAA, including the Privacy Rule and Security Rule (as defined in Article 1 of this Agreement), and with the applicable provisions of the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”).

b. Covered Entity has engaged Business Associate to furnish certain services to Covered Entity pursuant to a separate Business Services Agreement.

c. Business Associate is a business associate under HIPAA. Business Associate must comply with the provisions of the Privacy Rule and Security Rule made applicable to business associates pursuant to HITECH and with all other applicable provisions of HITECH and HIPAA.

d. Covered Entity is not permitted to allow Business Associate to create, receive, maintain, or transmit Protected Health Information on behalf of Covered Entity without satisfactory assurances that Business Associate will appropriately safeguard the information. Therefore, Covered Entity will only disclose Protected Health Information to Business Associate or allow Business Associate to create or receive Protected Health Information on behalf of Covered Entity in accordance with the requirements of HIPAA, HITECH, applicable state law, and the provisions of this Agreement.

NOW, THEREFORE, in consideration of the mutual promises below and for other good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, the parties agree as follows:

## Definitions

1. "Breach" shall have the same meaning as the term "breach" set out in 45 CFR 164.402.
2. "Business Associate" shall have the same meaning as the term under HIPAA, including, but not limited to, 45 CFR 160.103, and in reference to the party to this agreement, shall mean <insert company name>.
3. "CFR" means the Code of Federal Regulations. A reference to a CFR section means that section as amended from time to time; provided that if future amendments change the designation of a section referred to herein, or transfer a substantive regulatory provision referred to herein to a different section, the section references herein shall be deemed to be amended accordingly.
4. "Compliance Date(s)" shall mean the date(s) established by the Secretary or the United States Congress as the effective date(s) of applicability and enforceability of the Privacy Rule, Security Rule and HITECH Standards.
5. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR §164.501 and shall include a group of records that is: (i) the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for Covered Entity or (2) used, in whole or in part, by or for Covered Entity to make decisions about Individuals.
6. "Electronic Protected Health Information" (EPHI) shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to the information received from, or created on behalf of, Covered Entity by Business Associate.
7. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, as amended, and related HIPAA regulations (45 C.F.R. Parts 160-164).
8. “HITECH” means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005 and related regulations.
9. "HITECH Standards" shall mean the privacy, security and security breach notification provisions applicable to a Business Associate under Subtitle D of the Health Information Technology for Education and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009, and any regulations promulgated thereunder.
10. "Individual" shall have the same meaning as the term "individual" in 45 CFR

§160.103, and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

1. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and 164, subparts A and E.
2. "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information received from, or created on behalf of, Covered Entity by Business Associate.
3. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR §164.103.
4. "Security Incident" shall have the same meanings as the term "security incident" in 45 CFR §164.304.
5. "Security Rule" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR parts 160 and 164, subparts A and C. Terms used, but not otherwise defined, shall have the same meaning as those terms in the Privacy Rule, Security Rule and HITECH Standards.

## Obligations of Business Associate

* 1. Business Associate agrees not to use or disclose PHI other than as permitted or required by this Agreement or as Required by Law. Business Associate will take reasonable efforts to limit requests for, use and disclosure of PHI to the minimum necessary to accomplish the intended request, use or disclosure and comply with 45 CFR 164.502(b) and 514(d).
  2. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical, and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule.
  3. Business Associate agrees to report to Covered Entity any use or disclosure of PHI, other than as provided for by this Agreement, promptly after Business Associate has actual knowledge of such use or disclosure, and to report promptly to the Covered Entity all Security Incidents of which it becomes aware as determined by Business Associate except that, for purposes of this Security Incident reporting requirement, the term "Security Incident" shall not include unsuccessful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information

system of which it becomes aware as determined by Business Associate. Following the discovery of a breach of unsecured PHI, Business Associate shall notify Covered Entity of such breach without unreasonable delay, and in no event later than thirty (30) calendar days after such discovery. The notification will include the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed during the breach. A breach shall be treated as discovered as of the first day on which such breach is known or reasonably should have been known to Business Associate. Any notices required to be delivered by Covered Entity hereunder shall be at the expense of the Business Associate. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this agreement or applicable regulations.

* 1. Business Associate agrees to ensure access to ePHI is limited to workforce members who require such access because of their role or function.
  2. Business Associate agrees to implement safeguards to prevent its workforce members who are not authorized to have access to such ePHI from obtaining access and to otherwise ensure compliance by its workforce with the Security Rule
  3. Within fifteen (15) business days of receiving a request from Covered Entity, Business Associate agrees to implement restrictions on use or disclosure of PHI agreed to by the Covered Entity on behalf of an Individual in accordance with 45 CFR 164.522(a).
  4. Within fifteen (15) business days of receiving a request from Covered Entity, Business Associate agrees to honor requests for alternative communications agreed to by Covered Entity on behalf of an individual in accordance with 45 CFR 164.522(b).
  5. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, Business Associate agrees to ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information, including agreeing in writing to implement the same reasonable and appropriate safeguards that apply to Business Associate to protect the Covered Entity's ePHI.
  6. If Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to make available to Covered Entity, within a reasonable time, such information as Covered Entity may require to fulfill Covered Entity's obligations to respond to a request for access to PHI as provided under 45 CFR §164.524 or to respond to a request to amend PHI as required under 45 CFR §164.526. Business Associate shall refer to Covered Entity all such requests that Business Associate may receive from Individuals. If Covered Entity requests Business Associate to amend PHI in Business Associate's possession in order to comply with 45 CFR §164.526, Business Associate shall effectuate such amendments no later than the date they are required to be made by 45 CFR §164.526; provided that if Business Associate receives such a request from Covered Entity less than ten (10) business days prior to such date, Business Associate will effectuate such amendments as soon as is reasonably practicable.
  7. If applicable, Business Associate agrees to provide to Covered Entity, within a reasonable time, such information necessary to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures as provided under 45 CFR §164.528. Business Associate shall refer to Covered Entity all such requests which Business Associate may receive from individuals.
  8. Upon reasonable notice, Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the U.S. Secretary of Health and Human Services, or an officer or employee of that Department to whom relevant authority has been delegated, at Covered Entity's expense in a reasonable time and manner, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

l. Notwithstanding any other provision in this agreement, Business Associate hereby acknowledges and agrees that to the extent it is functioning as a Business Associate of Covered Entity, Business Associate will comply with the HITECH Business Associate provisions and with the obligations of a Business Associate as prescribed by HIPAA and the HITECH Act. Business Associate and the Covered Entity further agree that the provisions of HIPAA and the HITECH Act that apply to Business Associates, and that are required to be incorporated by reference in a Business Associate Agreement, are incorporated into this agreement between Business Associate and Covered Entity as if set forth in this agreement in their entirety.

## III. Permitted uses and disclosures by Business Associate

Except as otherwise limited in this Agreement, Business Associate may:

1. Use or disclose PHI on behalf of the Covered Entity, if such use or disclosure of PHI would not violate the Privacy Rule, including the minimum necessary standard, if done by the Covered Entity.
2. Use or disclose PHI to perform the services outlined in any and all services agreements, or other contracts, entered into between Covered Entity and Business Associate.
3. Use PHI for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate.
4. Disclose PHI for the proper management and administration of Business Associate, or to fulfill any present or future legal responsibilities of Business Associate, provided that such disclosure is either required by law or Business Associate obtains reasonable assurances from any person to whom PHI is disclosed that such person will: (i) keep such information confidential, (ii) use or further disclose such information only for the purpose for which it was disclosed to such person or as required by law, and (iii) notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
5. Use PHI to provide data aggregation services relating to the health care operations of the Covered Entity, as provided in 45 CFR §164.501.
6. To create de-identified data, provided that the Business Associate de-identifies the information in accordance with the Privacy Rule. De-identified information does not constitute PHI and is not subject to the terms and conditions of this Agreement.
7. Business Associate may use PHI to report violations of law to appropriate Federal and authorities, consistent with 45 CFR 164.5020)(1).

## Obligations of Covered Entity

* 1. Covered Entity shall notify Business Associate of any facts or circumstances that affect Business Associate's use or disclosure of PHI. Such facts and circumstances include, but are not limited to: (i) any limitation or change in Covered Entity's notice of privacy practices, (ii) any changes in, or withdrawal of, an authorization provided to Covered Entity by an Individual pursuant to 45 CFR §164.508; and (iii) any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522.
  2. Covered Entity agrees that it will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or is not otherwise authorized or permitted under this Agreement.
  3. Covered Entity acknowledges and agrees that the Privacy Rules allow the Covered Entity to permit Business Associate to disclose or provide access to PHI, other than Summary Health Information, to the Plan Sponsor only after the Plan documents have been amended to provide for the permitted and required uses and disclosures of PHI and to require the Plan Sponsor to provide a certification to the Plan that certain required provisions have been incorporated into the Plan documents before the Plan may disclose, either directly or through a Business Associate, any PHI to the Plan Sponsor.
  4. Covered Entity agrees that it will have entered into Business Associate Agreements with any third parties to whom Covered Entity directs and authorizes Business Associate to disclose PHI.

## Effective date: termination

* 1. The effective date of this agreement shall be the date this agreement is signed by both parties.
  2. This agreement shall terminate on the date Business Associates ceases to be obligated to perform the functions, activities, and services described in Article Ill Sections A and B.
  3. Upon Covered Entity's knowledge of a material breach by Business Associate of this Agreement, Covered Entity shall notify Business Associate of such breach and Business Associate shall have thirty (30) days to cure such breach. In the event Business Associate does not cure the breach, or cure is infeasible, Covered Entity shall have the right to immediately terminate this Agreement and any underlying services agreement. If cure of the material breach is infeasible, Covered Entity shall report the violation to the Secretary.
  4. Upon termination of this agreement, Business Associate will return to Covered Entity, or if return is not feasible, destroy, any and all PHI that it created or received on behalf of Covered Entity in a format selected by Covered Entity and retain no copies thereof. If the return or destruction of the PHI is determined by Business Associate not to be feasible, or if Business Associate is required by law to retain such information or copies thereof, Business Associate will maintain the PHI for the period of time required under applicable law, or in accordance with Business Associate's internal record retention schedule as in effect from time to time, whichever is longer, after which time Business Associate shall return or destroy the PHI.
  5. Business Associate's obligations under Sections II and Ill above shall survive the termination of this agreement with respect to any PHI so long as it remains in the possession of Business Associate.

1. **Other provisions**
   1. The parties acknowledge that the foregoing provisions are designed to comply with the mandates of the Privacy Rule, Security Rule, and the HITECH Standards. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law. If the parties are unable to reach agreement regarding an amendment within thirty (30 days) of the date that Business Associate receives any written objection from Covered Entity, either party may terminate this Agreement upon ninety (90) days written notice to the other party. Any other amendment to the Agreement unrelated to compliance with applicable law and regulations shall be effective only upon execution of a written agreement between the parties.
   2. Except as it relates to the use, security and disclosure of PHI and electronic transactions, this agreement is not intended to change the terms and conditions, or the rights and obligations, of the parties under any other services agreement between them.
   3. Business Associate agrees to defend, indemnify and hold harmless Covered Entity, its affiliates and its directors, officers, employees, agents or assigns from and against any and all actions, causes of action, claims, suits and demands whatsoever, and from all damages, liabilities, costs, charges, debts, fines, government investigations, proceedings, and expenses whatsoever (including reasonable attorneys' fees and expenses related to any litigation or other defense of any claims), which may be asserted, or for which it may now or hereafter become subject, arising in connection with (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on its part under this agreement; and (ii) any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of, or in any way connected with, Business Associate's performance under this agreement.
   4. In addition to the insurance required under the Agreement, Contractor at its sole cost and expense will obtain, keep in force, and maintain an insurance policy (or policies) that provides coverage for privacy and data security breaches. This specific type of insurance is typically referred to as Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability. In some cases, Professional Liability policies may include some coverage for privacy and/or data breaches. Regardless of the type of policy in place, it needs to include coverage for reasonable costs in investigating and responding to privacy and/or data breaches with the following minimum limits unless AU specifies otherwise: $1,000,000 Each Occurrence and $5,000,000 Aggregate.
   5. Nothing express or implied in this agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
   6. Any ambiguity in this agreement shall be resolved in favor of a meaning that permits the Covered Entity to comply with the Privacy Rule, Security Rule, and the HITECH Standards.
   7. If any provision of this Agreement is held illegal, invalid, prohibited, or unenforceable by a court of competent jurisdiction, that provision shall be limited or eliminated in that jurisdiction to the minimum extent necessary so that this agreement shall otherwise remain in full force and effect and enforceable.
   8. This Agreement shall be governed by and construed in accordance with the laws of the state of Alabama to the extent not preempted by the privacy or security or other applicable federal law.
   9. This Agreement replaces and supersedes in its (their) entirety any prior Business Associate Agreement(s) between the parties.

In witness whereof, this agreement has been signed and delivered as of the date first set forth above.

**AUBURN UNIVERSITY <insert company name>**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**By: Courtney Raville, Contract Officer By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**