

**BUSINESS ASSOCIATE AGREEMENT  
BETWEEN  
LEWIS & CLARK COLLEGE  
AND  
ALLEGIANCE BENEFIT PLAN MANAGEMENT, INC.**

**I. PREAMBLE**

Lewis & Clark College and Allegiance Benefit Plan Management, Inc., (jointly “the Parties”) wish to enter into this Business Associate Agreement (“Agreement”) to comply with the requirements of: (i) the implementing regulations at 45 CFR Parts 160, 162 and 164 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)(i.e., the HIPAA Privacy, Security, Electronic Transaction, Breach Notification and Enforcement Rules (“the Regulations”)) , (ii) the requirements of the Health Information Technology for Economic and Clinical Health Act, as set forth in the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”) that are applicable to business associates and (iii) the requirements of the final modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules as issued on January 25, 2013 and effective March 26, 2013 (75 Fed. Reg. 5566 (Jan. 25, 2013)) (the Final Regulations”). The Implementing Regulations, the HITECH Act, and the Final Regulations are collectively referred to in this Agreement as the “HIPAA Requirements.”

Covered Entity and Business Associate agree to incorporate into this Agreement any regulations issued by the US Department of Health and Human Services (“DHHS”) with respect to the HIPAA requirements that relate to the obligations of business associates and that are required to be reflected in a business associate agreement. Business Associate recognizes and agrees that it is obligated by law to meet the applicable provisions of the HIPAA Requirements and that it has direct liability for any violations of the HIPAA Requirements. The services to be provided by Business Associate are identified in a separate agreement between the Parties entitled Administrative Services Agreement.

**II. DEFINITIONS**

- A. “*Breach*” shall mean, as defined in 45 CFR § 164.402, the acquisition, access use or disclosure of Unsecured Protected Health Information in a manner not permitted by the HIPAA Requirements that compromises the security or privacy of that Protected Health Information.
- B. “*Business Associate Subcontractor*” shall mean, as defined in 45 CFR § 164.103, any entity (including an agent) that creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate.
- C. “*Electronic PHI*” shall mean, as defined in 45 CFR § 160.103, Protected Health Information that is transmitted or maintained in any Electronic Media.
- D. “*Limited Data Set*” shall mean, as defined in 45 CFR § 164.514(e) Protected Health Information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
  - (i) Names;
  - (ii) Postal address information, other than town or city, state, and zip code;
  - (iii) Telephone numbers;
  - (iv) Fax numbers;
  - (v) Electronic mail addresses;
  - (vi) Social security numbers;
  - (vii) Medical record numbers;
  - (viii) Health plan beneficiary numbers;
  - (ix) Account numbers;
  - (x) Certificate/license numbers;

- (xi) Vehicle identifiers and serial numbers, including license plate numbers
  - (xii) Device identifiers and serial numbers;
  - (xiii) Web Universal Resource Locators (URLs);
  - (xiv) Internet Protocol (IP) address numbers;
  - (xv) Biometric identifiers, including finger and voice prints; and
  - (xvi) Full face photographic images and any comparable images.
- E. “*Protected Health Information*” or “*PHI*” shall mean, as defined in 45 CFR § 164.103, information created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse, that: (i) relates to the past, present, or future physical or mental health or condition of an individual, provision of health care to the individual, or the past, present, or future payment for provision of health care to the individual; (ii) identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and (iii) is transmitted or maintained in an electronic medium, or in any other form or medium. The use of the term “Protected Health Information” or “PHI” in this Agreement shall mean both Electronic PHI and non-electronic PHI, unless another meaning is clearly specified.
- F. “*Security Incident*” shall mean, as defined in 45 CFR § 164.304, the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- G. “*Unsecured Protected Health Information*” shall mean, as defined in 45 CFR § 164.402, Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by DHHS.
- H. All other capitalized terms used in this Agreement shall have the meanings set forth in the applicable definitions under the HIPAA Requirements.

### **III. GENERAL TERMS**

- A. In the event of an inconsistency between the provisions of this Agreement and a mandatory term of the HIPAA Requirements (as these terms may be expressly amended from time to time by the DHHS or as a result of interpretations by DHHS, a court, or another regulatory agency having regulatory authority over the Parties, the interpretation of DHHS, such court or regulatory agency shall prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with the rules of precedence.
- B. Where provisions of this Agreement are different from those mandated by the HIPAA Requirements, but are nonetheless permitted by the HIPAA Requirements, the provisions of this Agreement shall control.
- C. Except as expressly provided in the HIPAA Requirements or this Agreement, this Agreement does not create any rights in third parties.

### **IV. SPECIFIC REQUIREMENTS OF BUSINESS ASSOCIATE**

- A. Flow-down of Obligations to Business Associate Subcontractors.

Business Associate agrees that as required by the HIPAA Requirements, Business Associate will enter into a written agreement with all Business Associate Subcontractors that: (i) requires them to comply with the Privacy and Security Rule provisions of this Agreement in the same manner as required of Business Associate, and (ii) notifies such Business Associate Subcontractors that they will incur liability under the HIPAA Requirements for non-compliance with such provisions. Accordingly, Business Associate shall ensure that all Business Associate Subcontractors agree in

writing to the same privacy and security restrictions, conditions and requirements that apply to Business Associate with respect to PHI.

B. Privacy of Protected Health Information

1. *Permitted Uses and Disclosures of PHI.* Business Associate agrees to create, receive, use disclose, maintain or transmit PHI only in a manner that is consistent with this Agreement or the HIPAA Requirements and only in connection with providing the services to Covered Entity identified in the Agreement. Accordingly, in providing services to or for the Covered Entity, Business Associate, for example, will be permitted to use and disclose PHI for "Treatment, Payment and Healthcare Operations" as those terms are defined in the HIPAA Requirements. Business Associate further agrees that to the extent it is carrying out one or more of the Covered Entity's obligations under the Privacy Rule (Subpart E 45 CFR part 164), it shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.
  - (a) Business Associate shall report to Covered Entity any use or disclosure of PHI that is not provided for in this Agreement, including reporting Breaches of Unsecured Protected Health Information as required by 45 CFR § 160.410 and required by Section 4(e) (ii) below.
  - (b) Business Associate shall establish, implement and maintain appropriate safeguards and comply with the Security Standards (Subpart C of 45 CFR Part 164) with respect to Electronic PHI, as necessary to prevent any use or disclosure of PHI other than as provided for by this Agreement.
2. *Business Associate Obligations.* As permitted by the HIPAA Requirements, Business Associate also may use or disclose PHI received by the Business Associate in its capacity as a Business Associate to the Covered Entity for Business Associate's own operations if:
  - (a) the use relates to: (1) the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate, or (2) data aggregation services relating to the health care operations of the Covered Entity; or
  - (b) the disclosure of information received in such capacity will be made in connection with a function, responsibility, or services to be performed by the Business Associate, and such disclosure is required by law or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and the person agrees to notify the Business Associate of any breaches of confidentiality.
3. *Minimum Necessary Standard and Creation of Limited Data Set.* Business Associate's use, disclosure, or request of PHI shall utilize a Limited Data Set if practicable. Otherwise, in performing the functions and activities as specified in the separate agreement for services between the parties and this Agreement, Business Associate agrees to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request.
4. *Access.* In accordance with 45 CFR § 164.524 of the HIPAA Requirements, Business Associate will make available to the Covered Entity (or as directed by the Covered Entity, to those individuals who are the subjects of the PHI (or their designees)), their PHI in the Designated Record Set. Business Associate shall make such information available in an electronic format where directed by Covered Entity.
5. *Disclosure Accounting.* Business Associate shall make available the information necessary to provide an accounting of disclosures of PHI as provided for in 45 C.F.R. ' 164.528 of the HIPAA Requirements by making such information available to the Covered Entity or (at the direction of the Covered Entity) making such information available directly to the individual.

6. *Amendment.* Business Associate shall make available PHI in a Designated Record Set available for amendment and, as directed by the Covered Entity, incorporate any amendment to PHI in accordance with 45 C.F.R. ' 164.526 of the HIPAA Requirements.
7. *Right to Request Restrictions on the Disclosure of PHI and Confidential Communications.* If an individual submits a Request for Restriction or Request for Confidential Communications to the Business Associate, Business Associate and Covered Entity agree that Business Associate, on behalf of Covered Entity, will evaluate and respond to these requests according to Business Associate's own procedures for such requests.
8. *Return or Destruction of PHI.* Upon the termination or expiration of the agreement for services between the parties or this Agreement, Business Associate agrees to return the PHI to Covered Entity, destroy the PHI (and retain no copies), or if Business Associate determines that return or destruction of the PHI is not feasible (a) continue to extend the protections of this Agreement and of the HIPAA Requirements to the PHI, and (b) limit any further uses and disclosures of the PHI to the purpose making return or destruction infeasible.
9. *Availability of Books and Records.* Business Associate shall make available to DHHS or its agents the Business Associate's internal practices, books, and records relating to the use and disclosure of PHI in connection with this Agreement.
10. *Termination for Breach.*
  - (a) Business Associate agrees that Covered Entity shall have the right to terminate this Agreement or seek other remedies if Business Associate violates a material term of this Agreement.
  - (b) Covered Entity agrees that Business Associate shall have the right to terminate this Agreement or seek other remedies if Covered Entity violates a material term of this Agreement.

C. Information and Security Standards

1. Business Associate will develop, document, implement, maintain, and use appropriate Administrative, Technical, and Physical Safeguards to preserve the Integrity, Confidentiality, and Availability of, and to prevent non-permitted use or disclosure of, Electronic PHI created or received from or for the Covered Entity.
2. Business Associate agrees that with respect to Electronic PHI, these Safeguards, at a minimum, shall meet the requirements of the HIPAA Security Standards applicable to Business Associate.
3. To comply with the HIPAA Security Standards for Electronic PHI, Business Associate agrees that it shall:
  - (a) Implement Administrative, Physical and Technical Safeguards consistent with (and as required by) the HIPAA Security Standards that reasonably protect the Confidentiality, Integrity and Availability of Electronic PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate shall develop and implement policies and procedures that comply with the HIPAA Requirements;
  - (b) As also provided for in Section IV A. above, ensure that any Business Associate Subcontractor agrees to implement reasonable and appropriate safeguards to protect the Electronic PHI;
  - (c) Report to Covered Entity any unauthorized access, use, disclosure, modification, or destruction of PHI (including Electronic PHI) not permitted by this Agreement, applicable law,

or permitted by Covered Entity in writing (Successful Security Incidents or Breaches) of which Business Associate becomes aware. Business Associate shall report such Successful Security Incidents or Breaches to Covered Entity as specified in Section E. 3 (a) below

- (d) For Security Incidents that do not result in unauthorized access, use, disclosure, modification, or destruction of PHI (including for example and not limitation, pings on Business Associate's firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks, that do not result in the system being taken offline, or malware such as worms or viruses) (hereinafter "Unsuccessful Security Incidents"), aggregate the data and, upon the Covered Entity's written request, report to the Covered Entity in accordance with the reporting requirements identified in Section E. 3. (b);
- (e) Take all commercially reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to Business Associate resulting from any unauthorized access, use, disclosure, modification, or destruction of PHI;
- (f) Permit termination of this Agreement if the Covered Entity determines that Business Associate has violated a material term of this Agreement with respect to Business Associates security obligations and Business Associate is unable to cure the violation; and
- (g) Upon Covered Entity's request, provide Covered Entity with access to and copies of documentation regarding Business Associate's safeguards for PHI and Electronic PHI.

D. Compliance with HIPAA Transaction Standards

1. *Application of HIPAA Transaction Standards.* Business Associate will conduct Standard Transactions consistent with 45 CFR Part 162 for or on behalf of the Covered Entity to the extent such Standard Transactions are required in the course of Business Associate's performing services under the agreement for services and this Agreement for the Covered Entity. As provided for in Section IV A. above, Business Associate will require any Business Associate Subcontractor involved with the conduct of such Standard Transactions to comply with each applicable requirement of 45 CFR Part 162. Further, Business Associate will not enter into, or permit its Subcontractors to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of the Covered Entity that:
  - (a) Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;
  - (b) Adds any data element or segment to the maximum defined data set;
  - (c) Uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification or is not or is not in the Standard Transaction's implementation specification; or
  - (d) Changes the meaning or intent of the Standard Transaction's implementation specification.
2. *Specific Communications.* Business Associate, Plan Sponsor and Covered Entity recognize and agree that communications between the parties that are required to meet the Standards for Electronic Transactions will meet the standards set by that regulation. Communications between Plan Sponsor and Business Associate, or between Plan Sponsor and the Covered Entity, do not need to comply with the HIPAA Standards for Electronic Transactions. Accordingly, unless agreed otherwise by the Parties in writing, all communications (if any) for purposes of "Enrollment" as that term is defined in 45 CFR Part 162, Subpart O or for "Health Covered Entity Premium Payment Data" as that term is defined in 45 CFR Part 162, Subpart Q, shall be conducted between the Plan Sponsor and either Business Associate or Covered Entity. For all

such communications (and any other communications between Plan Sponsor and the Business Associate), Plan Sponsor shall use such forms, tape formats or electronic formats as Business Associate may approve. Plan Sponsor will include all information reasonably required by Business Associate to effect such data exchanges or notifications.

3. *Communications Between the Business Associate and the Covered Entity.* All communications between Business Associate and Covered Entity required to meet the HIPAA Standards for Electronic Transactions shall do so. For any other communications between Business Associate and Covered Entity, Covered Entity shall use such forms, tape formats, or electronic formats as Business Associate may approve. Covered Entity shall include all information reasonably required by Business Associate to affect such data exchanges or notifications.

E. Notice and Reporting Obligations of Business Associate

1. *Notice of Non-Compliance with the Agreement.* Business Associate shall notify Covered Entity within twenty (20) calendar days after discovery of any unauthorized access, use, modification or destruction of PHI (including any successful Security Incident) that is not permitted by this Agreement, by applicable law, or permitted in writing by Covered Entity, whether such non-compliance is by Business Associate or by a Business Associate Contractor.
2. *Notice of Breach.* Business Associate will notify Covered Entity following discovery and without unreasonable delay but in no event later than twenty (20) calendar days following discovery of any "Breach" of "Unsecured Protected Health Information" whether such breach is by Business Associate or by a Business Associate Contractor.
  - (a) As provided for in 45 CFR ' 164.402, Business Associate recognizes and agrees that any acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA privacy Rule (Subpart E of 45 CFR part 164) is presumed to be a Breach. As such, Business Associate shall (i) notify Covered Entity of any non-permitted acquisition, access, use or disclosure of PHI, and (ii) assist Covered Entity in performing (or at Covered Entity's direction, perform) a risk assessment to determine if there is a low probability that the PHI has been compromised.
  - (b) Business Associate shall cooperate with Covered Entity in meeting the Covered Entity's obligations under the HIPAA Requirements and any other security breach notification laws. Business Associate shall follow its notifications to the Covered Entity with a report that meets the requirements outlined immediately below.
3. *Reporting Obligations.*
  - (a) For Successful Security Incidents and Breaches, Business Associate ,--without unreasonable delay and in no event later than thirty (30) days after Business Associate learns of such non permitted use or disclosure (whether by Business Associate or by Business Associate's Contractor)—shall provide Covered Entity a report that will:
    - (1) Identify (if known) each individual whose Unsecured PHI has been or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed;
    - (2) Identify the nature of the non-permitted access, use, or disclosure including the date of the incident and the date of discovery;
    - (3) Identify the PHI accessed, used, or disclosed (e.g., name, SSN, DOB);
    - (4) Identify the corrective action Business Associate (or Business Associate Contractor) took or will take to prevent further non-permitted accesses, uses or disclosures;

(5) Identify what Business Associate (or Business Associate Contractor) did or will do to mitigate any deleterious effect of the non-permitted access, use or disclosure; and

(6) Provide any other information the Covered Entity may reasonably request.

(b) For Unsuccessful Security Incidents, Business Associate shall provide Covered Entity, upon its written request, a report that: (i) identifies the categories of Unsuccessful Security Incidents as described in Section 4(c)(iii)(d); (ii) indicates whether Business Associate believes its (or Business Associate Subcontractor's) current defensive security measures are adequate to address all Unsuccessful Security Incidents, given the scope and nature of such attempts; and (iii) if the security measures are not adequate, the measures Business Associate (or Business Associate Subcontractor) will implement to address the security inadequacies.

## V. TERM AND TERMINATION

- A. The Term of this Agreement shall be effective as of March 26, 2013 and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
- B. Covered Entity and Business Associate each have a right to terminate this Agreement if the other party has engaged in a pattern of activity or practice that constitutes a material breach or violation of Business Associate's or Covered Entity's respective obligations regarding PHI under this Agreement and, on notice of such material breach or violation from the Covered Entity or Business Associate, fails to take reasonable steps to cure the material breach or end the violation.
- C. If Business Associate or Covered Entity fail to cure the material breach or end the violation after the other party's notice, the Covered Entity or Business Associate (as applicable) may terminate this Agreement by providing Business Associate or the Covered Entity written notice of termination, stating the uncured material breach or violation that provides the basis for the termination and specifying the effective date of the termination. Such termination shall be effective 60 days from this termination notice.
- D. Business Associate's and the Covered Entity's obligations to protect the privacy and the security of the PHI it created, received, maintained, or transmitted in connection with services to be provided under the agreement for services between the parties and this Agreement will be continuous and survive termination, cancellation, expiration or other conclusion of this Agreement or the agreement for services. Business Associate's other obligations and rights and the Covered Entity's obligations and rights upon cancellation, expiration or other conclusion of this Agreement are those set forth in this Agreement or agreement for services between the parties.

IN WITNESS WHEREOF, the parties have caused this Business Associate Agreement to be executed on their behalf by their duly authorized representatives' signatures, effective as of the date first written above.

LEWIS & CLARK COLLEGE

TITLE:

BY: \_\_\_\_\_  
NAME:

ALLEGIANCE BENEFIT PLAN MANAGEMENT, INC.

BY: \_\_\_\_\_

NAME:  
TITLE: