

## **BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (“BAA”) is entered into by and between the *Arkansas Department of Finance and Administration, Employee Benefits Division* (“Covered Entity”) and the \_\_\_\_\_ (hereinafter “Business Associate”).

### **WITNESSETH:**

WHEREAS, the parties to this Business Associate Agreement have entered into an arrangement under which the Business Associate provides certain services to the Covered Entity as more fully described in the Agreement between the parties; and

WHEREAS, the Covered Entity will disclose certain information to the Business Associate during the course of the latter’s provision of such services, some of which may constitute “Protected Health Information” or “Electronic Protected Health Information,” as those terms are defined in federal regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), specifically 45 CFR Parts 160 and 164 (the “Privacy Rule” and “Security Rule”); and

WHEREAS, both the Business Associate and the Covered Entity intend to comply with HIPAA, the HITECH Act, and applicable Arkansas law in order to protect the privacy and to provide for the security of PHI and ePHI disclosed to the Business Associate; and

WHEREAS, both the Business Associate and the Covered Entity wish to set forth the terms and the conditions pursuant to which PHI and ePHI received by the Business Associate in the performance of services for the Covered Entity will be handled between themselves and with third parties in compliance with HIPAA and the HITECH Act;

NOW, THEREFORE, in consideration of the mutual promises, covenants, terms, and conditions contained herein, and intending to be legally bound, the Business Associate and the Covered Entity agree as follows:

#### **1. Definitions.**

The following terms shall be defined as set forth below. Terms used, but not defined in this Agreement, shall have the same meaning as those terms in the Privacy Rule and Security Rule.

- (a) For purposes of this Agreement, “Business Associate” shall mean the named Business Associate hereinabove.

- (b) For purposes of this Agreement, “Covered Entity” shall include the named Covered Entity hereinabove, as well as any other entity specifically identified in any joint notice of privacy practices utilized pursuant to the Privacy Rules.
- (c) “Electronic Protected Health Information” or “ePHI” shall have the same meaning as that term is defined at 45 CFR § 160.103, limited to the information received by the Business Associate from or on behalf of the Covered Entity.
- (d) “HIPAA” shall mean the Health Insurance Portability and Accountability Act of 1996.
- (e) “HITECH Act” shall mean the Health Information Technology for Economic and Clinical Health Act.
- (f) “Individual” shall have the same meaning as that term is defined at 45 CFR § 160.103, and shall include a person who qualifies as a personal representative of an Individual in accordance with 45 CFR § 164.502(g).
- (g) “Limited Data Set” shall have the same meaning as that term is defined at 45 CFR § 164.514 (e).
- (h) “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information promulgated at 45 CFR Part 160 and Part 164, Subparts A, D, and E, and any other applicable provision of HIPAA, and any amendments thereto, including HITECH.
- (i) “Protected Health Information” or “PHI” shall have the same meaning as that term is defined at 45 CFR § 160.103, limited to the information received or created by the Business Associate from or on behalf of the Covered Entity. Unless otherwise stated in this Agreement, any provision, restriction, or obligation in this Agreement related to the use or disclosure of PHI shall apply equally to ePHI.
- (j) “Required by Law” shall have the same meaning as that term is defined at 45 CFR § 164.103.
- (k) “Secretary” shall mean the Secretary of the Department of Health and Human Services, or his or her designee.
- (l) “Security Breach” shall have the same meaning as the term “Breach” is defined at 45 CFR § 164.402, and shall mean the acquisition, access, use, or disclosure of PHI or ePHI in a manner not permitted under the Privacy Rule and which compromises the security or privacy of the PHI or ePHI.
- (m) “Security Incident” shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as provided in 45 CFR § 164.304, except that “Security Incident” shall not include unsuccessful spam emails, viruses, phishing scams, firewall attacks, DOS or DDOS attacks, or any other unsuccessful attempted unauthorized activity or interference if such activity or interference is sufficiently common or routine to be successfully neutralized in the ordinary course of providing data security.
- (n) “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information promulgated at 45 CFR Part 160 and Part 164, Subpart C, and any other applicable provision of HIPAA, and any amendments thereto, including HITECH.

- (o) “Unsecured PHI” shall mean PHI or ePHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued pursuant to § 13402 of the HITECH Act, as provided in 45 CFR § 164.402.

## **2. Background of the Agreement**

The Business Associate and the Covered Entity have entered into an Agreement for services. In the performance of these services, the Covered Entity may disclose PHI to the Business Associate. The Business Associate acknowledges that certain sections of the Privacy Rule and the Security Rule, as well as the HITECH Act, apply directly to the Business Associate as they apply to the Covered Entity. Both parties are committed to complying with the Privacy Rule and Security Rule under HIPAA, as amended by the HITECH Act, and accordingly, have entered into this Agreement to set forth the terms and conditions of how such PHI shall be handled between the Business Associate, the Covered Entity, and third parties. The parties have entered into this BAA in order to set forth the terms and conditions for access to and use of the PHI and ePHI.

## **3. Permitted Uses and Disclosures by the Business Associate**

- (a) Except as otherwise limited in this Agreement, the Business Associate may use or disclose PHI on behalf of the Covered Entity for purposes of providing the services described hereinabove and described in any written agreement between the parties, provided that such use or disclosure shall not violate HIPAA, the HITECH Act, the Privacy Rule, or Security Rule if done by the Covered Entity. Except as otherwise limited in this Agreement, the Business Associate may use PHI for the proper management and administration of the Business Associate, or to carry out the legal responsibilities of the Business Associate.
- (b) Except as otherwise limited in this BAA, the Business Associate may disclose PHI to a third person for the proper management and administration of the Business Associate, provided that such disclosures are Required By Law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and may only be used or further disclosed as Required By Law, or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been the subject of a Security Breach.
- (c) The Business Associate may use PHI to report violations of law to appropriate federal and state authorities in accordance with 45 CFR § 164.502(j)(1).
- (d) The Business Associate may de-identify any and all PHI that it obtains from the Covered Entity, but only if such de-identification is accomplished in accordance with the requirements of 45 CFR § 514 (a) and (b).
- (e) The Business Associate may use and disclose PHI only if such use and disclosure is in compliance with each applicable requirement of 45 CFR § 164.504(e).

#### **4. Obligations of the Business Associate**

- (a) The Business Associate agrees not to use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.
- (b) The Business Associate agrees to use appropriate safeguards to prevent disclosure of the PHI other than as provided for by this Agreement, and to implement administrative, physical, and technical safeguards as required by 45 CFR §§ 164.308, 164.310, 164.312, and 164.316 in order to protect the confidentiality, integrity, and availability of PHI that the Business Associate receives, maintains, or transmits to the same extent as if the Business Associate were a Covered Entity. The Business Associate shall undertake such actions in a manner that is consistent with any guidance issued by the Secretary pursuant to the HITECH Act.
- (c) The Business Associate agrees to report to the Covered Entity within five (5) business days of becoming aware of any use or disclosure of PHI not provided for by this Agreement. In addition, the Business Associate shall notify the Covered Entity of any Security Incident or Security Breach. This notice shall include the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been accessed, acquired or disclosed during the Security Breach, analysis of the storage mechanisms for the PHI, the data elements that have been compromised, and all details regarding the circumstances by which the PHI came to be compromised. The Business Associate agrees to cooperate with the Covered Entity in mitigating, to the extent practicable, any harmful effect that is known to exist as a result of such unauthorized use or disclosure of PHI, such Security Incident, or Security Breach. The Business Associate further agrees to cooperate with the Covered Entity in complying with all state and federal public notification requirements arising therefrom.
- (d) The Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from or received by the Business Associate on behalf of the Covered Entity, agrees to the same restrictions and conditions that apply in the Agreement to the Business Associate with respect to such information, including but not limited to, the requirement that such agent or subcontractor implement reasonable and appropriate safeguards to protect such information.
- (e) The Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI received from or received by the Business Associate on behalf of the Covered Entity, available to the Covered Entity, or at the request of the Covered Entity, to the Secretary, for purposes of determining the Covered Entity's and/or the Business Associate's compliance with HIPAA, the HITECH Act, the Privacy Rule, or the Security Rule.
- (f) In the event that the parties mutually agree that the PHI received from or received by the Business Associate on behalf of the Covered Entity constitutes a Designated Records Set, the Business Associate agrees to refer any requests from an Individual for amendment of that individual's PHI pursuant to 45 CFR § 164.526 to the Covered Entity. The Business Associate agrees to notify the Covered Entity of any such requests within five (5) business days of receiving them. Amendment of an Individual's PHI is the sole responsibility of the Covered Entity.

- (g) The Business Associate shall only request, use, or disclose the minimum amount of PHI necessary to accomplish the intended purpose of the request, use, or disclosure. The Business Associate agrees to comply with the Secretary's guidance issued pursuant to the HITECH Act as to what constitutes "Minimum Necessary".

**5. Obligations of the Covered Entity**

- (a) The Covered Entity shall immediately notify the Business Associate of any limitations in the Notice of Privacy Practices maintained by the Covered Entity to the extent that such limitations may affect the Business Associate's use or disclosure of the PHI.
- (b) The Covered Entity shall immediately notify the Business Associate of any changes in, or revocation of permission granted by an Individual under 45 CFR § 164.506 or § 164.508 to use or disclose PHI, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.
- (c) The Covered Entity shall immediately notify the Business Associates of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR § 164.522 to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- (d) The Covered Entity shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rules if done by the Covered Entity.

**6. Term.**

The term of this Agreement shall remain in force and effect until terminated pursuant to Section 7 herein below.

**7. Termination.**

- (a) If the Covered Entity determines that the Business Associate has breached a material term of this BAA, the Covered Entity shall provide written notice of the material breach to the Business Associate, after which the Business Associate shall have thirty (30) days to take reasonable steps to cure the breach. If the Business Associate does not cure the breach within this specified time, the Covered Entity may terminate this BAA and any related agreements covering the services provided by the Business Associate to or on behalf of the Covered Entity. If neither cure nor termination is feasible, the Covered Entity shall report the breach to the Secretary.
- (b) The Business Associate may terminate this BAA for any reason upon thirty (30) days' notice to the Covered Entity.
- (c) Either party may terminate this BAA when all the PHI received from or received by the Business Associate on behalf of the Covered Entity is destroyed or returned to the Covered Entity, or if it is infeasible to return or destroy the PHI, the protections are extended to such information in accordance with the provisions of Section 7(d) and (e) herein below.
- (d) Subject to the provisions of Section 7(e) herein below, upon termination of this Agreement for any reason, the Business Associate shall return or destroy all PHI received from, or created or received by the Business Associate on behalf of the Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of the

Business Associate and the Business Associate shall so notify its subcontractors or agents of these obligations. The Business Associate and its subcontractors or agents shall retain no copies of the PHI.

- (e) In the event that the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the Covered Entity notification of the conditions that make the return or destruction of such information infeasible. Upon such notification, the Business Associate shall extend the protections of this Agreement to such PHI, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI. In the event that it is infeasible for the Business Associate to obtain from a subcontractor or agent of the Business Associate any PHI in the possession of the subcontractor or agent, the Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction of such information from the subcontractor or agent infeasible. Upon such notification, the Business Associate shall require the subcontractor or agent to extend the protections of this BAA to such PHI, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the subcontractor or agent maintains such PHI.
- (f) This BAA will automatically terminate without any further action of the parties upon the termination of the services provided by the Business Associate to or behalf of Covered Entity.

**8. Regulatory References.**

Any reference in this BAA to a provision of the Privacy Rule or Security Rule shall mean the section as in effect or as amended.

**9. Survival.**

The respective rights and obligations of the Business Associate under Section 7(d) and (e) of this Agreement shall survive the termination of this Agreement.

**10. No Third-Party Beneficiaries.**

Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person, other than the parties and their respective successors and assigns, any rights, remedies, obligations, or liabilities whatsoever.

**11. Disputes.**

If any dispute or claim arises between the parties with respect to this Agreement, the parties will make a good faith effort to resolve such matters informally, it being the intention of the parties that they reasonably cooperate with each other in the performance of the mutual obligations under this Agreement.

**12. Amendment.**

The parties agree to take such action as is necessary to amend this Agreement from time to time in order for the Covered Entity to comply with the requirements of HIPAA and the HITECH Act, as those statutes and their implementing regulations may be amended from time

to time. No amendment to this Agreement shall be effective until reduced to writing and duly signed by the authorized representatives of the parties.

**13. Non-Waiver.**

A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any other right or remedy as to any subsequent events.

**14. Assignment.**

Neither party may assign any of its rights or obligations under this Agreement without the prior written consent of the other party.

**15. Nature of Agreement.**

Nothing in this Agreement shall be construed to create a partnership, joint venture, or other joint business relationship between the parties or any of their affiliates, or a relationship of employer and employee between the parties. Rather, it is the intention of the parties that their relationship shall be that of independent contractors.

**16. Entire Agreement.**

This Agreement constitutes the entire agreement between the Business Associate and the Covered Entity relating to the matters specified in this Agreement, and supersedes all prior representations or agreements, whether oral or written, with respect to such matters.

**17. Severability.**

Any provision of this Agreement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity of enforceability of such remaining provisions.

**18. Notices.**

All notices, requests, demands, and other communications required or permitted to be given under this Agreement shall be in writing, and shall be effective upon receipt. Such notice may be made by personal delivery, by overnight delivery service with proof of delivery, or by certified or registered United States mail, return receipt requested. All such communications shall be sent to the addresses of the other party as set out in the signature blocks below. Neither party shall refuse delivery of any notice hereunder.

**19. Interpretation.**

Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA and the HITECH Act, as those statutes and their implementing regulations may be amended from time to time. The provisions of this Agreement shall prevail over any provision of any other agreement between the Business Associate and the Covered Entity that may conflict or be inconsistent with any provisions in this Agreement.

**20. Governing Law, Jurisdiction and Venue.**

This Agreement and the rights and obligations of the parties hereunder shall be construed, interpreted, and enforced with, and shall be governed by, the laws of Arkansas.

**21. Counterparts.**

This Agreement may be executed in one or more counterparts, each of which shall be deemed and original, but all of which together shall constitute one and the same document.

**The parties have executed this Agreement as of the date signed below.**

**For Business Associate:**

**For Covered Entity:**

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Chris Howlett, Executive Director  
Employee Benefits Division - DFA  
501 Woodlane, Suite 500  
Little Rock, AR 72201  
Office: 501.682.5502

\_\_\_\_\_  
Title

\_\_\_\_\_  
Address

\_\_\_\_\_  
City, State, Zip Code

\_\_\_\_\_  
Date Signed