

## **Supplement Six – Business Associate Agreement**

## BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT is entered into this \_\_\_\_ day of \_\_\_\_\_, \_\_\_\_\_, by and between \_\_\_\_\_ (referred to as "Business Associate") and the State of Ohio, Department of Administrative Services (referred to as "Agency"), for length of underlying agreement.

WHEREAS, Agency will make available and/or transfer to Business Associate confidential, personally identifiable health information in conjunction with the terms and conditions of the underlying agreement, and

WHEREAS, such information may be used or disclosed only in accordance with the privacy regulations [45 CFR §§ 164.502(e); 164.504(e)] and the security regulations [45 CFR §§ 164.308; 164.314] issued pursuant to the Health Insurance Portability and Accountability Act [42 USC §§ 1320 - 1320d-8], relevant amendments effected by the American Recovery and Reinvestment Act of 2009 [Pub. L. 111-5, §§ 13400 *et seq.*] and the terms of this Agreement, or more stringent provisions of the law of the State of Ohio;

NOW THEREFORE, the parties agree as follows:

### 1. Definitions.

- 1.1. **Protected Health Information ("PHI")** means individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual, as more fully defined in 45 CFR § 164.501, and any amendments thereto, received from or on behalf of the Agency.
- 1.2. **Unsecured PHI** is PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.
- 1.3. **Business Associate** shall have the meaning given to such term in 45 CFR § 160.103.
- 1.4. **Individual** means the person who is the subject of the PHI, as defined in 45 CFR § 160.103, and includes the person's personal representative.
- 1.5. **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and Part 164, Subparts A and E, and any amendments thereto.

2. **Copy of Privacy Practices.** If applicable, Agency shall provide to the Business Associate a copy of the current Notice of Privacy Practices and any relevant information on changes to or agreed upon restrictions relating to legal permissions for the use or disclosure of PHI.

3. **Permitted Use.** The Business Associate agrees that it shall not receive, create, use or disclose PHI except as follows:

- 3.1. **Covered Functions.** Except as otherwise limited in this Agreement, Business Associate may use or disclose the PHI on behalf of, or to provide services to,

Agency for the purposes necessary to complete the tasks, or provide the services, associated with, and required by the terms of the underlying agreement.

**3.2. Disclosure Restrictions.** If necessary for the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate. PHI may only be disclosed to another person/entity for such purposes if:

3.2.1. Disclosure is required by law; or

3.2.2. Where the Business Associate obtains reasonable assurances from the person to whom disclosure is made that the PHI released will be held confidentially and only may be used or further disclosed as required by law or for the purposes of the disclosure; and person/entity agrees to notify Business Associate of any breaches of confidentiality in a timely fashion and in writing. Documentation needs to follow the same standards and time frames as item 6 below.

**3.3. Data Aggregation.** To permit the Business Associate to provide data aggregation services relating to the operations of Agency. Aggregation is defined as combining PHI received from multiple Business Associates to produce data analysis that relates to the operation of the respective Covered Entities.

**4. Minimize Use of PHI.** The Business Associate agrees that it will not request, use or release more than the minimum necessary amount of PHI to accomplish the purpose of the use, disclosure or request.

**5. Business Associate Safeguards.** The Associate will use appropriate safeguards to prevent any unauthorized use or disclosure of PHI and shall implement the administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of the PHI that it creates, receives, maintains or transmits on behalf of the Agency. The Associate will use all appropriate safeguards under 45 CFR 164 Subpart C including those identified as addressable. The Associate will comply with 74 FR 19006 Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII. With regard to electronic PHI not covered by the Guidance published at 74 FR 19006, the Associate will protect electronic PHI at rest and in transit through encryption that complies with State of Ohio IT Standard, ITS-SEC-01 Data Encryption and Cryptography.

**6. Unauthorized Disclosure and Incident Reporting and Remediation and Privacy and Security Breach Notification.**

**6.1. Incident Reporting.**

6.1.1. Business Associate shall report to Covered Entity the following:

6.1.1.1. Any use or disclosure of PHI which is not in compliance with the terms of this Agreement or applicable law of which it becomes aware; and

6.1.1.2. Any security incident of which it becomes aware. For purposes of this Agreement, "security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

6.1.2. Within 24 hours of discovery of a suspected reportable incident as described in 6.1.1 above, Business Associate shall notify Covered Entity of the existence and nature of the incident as understood at that time. Business Associate shall immediately investigate the incident and within 72 hours of discovery shall provide Covered Entity, in writing, a report describing the results of Business Associate's investigation, including:

6.1.2.1. What data elements were involved, the extent of the data involved in the incident, and the identification of affected individuals, if applicable;

6.1.2.2. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI, or to have been responsible for the incident;

6.1.2.3. A description of where the PHI is believed to have been improperly transmitted, sent, or utilized, if applicable;

6.1.2.4. A description of the probable causes of the incident;

6.1.2.5. A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval; and

6.1.2.6. Whether the Associate believes any federal or state laws requiring notifications to individuals are triggered.

6.1.3. Reporting and other communications made to the Covered Entity under this section must be made to the agency's HIPAA privacy officer at:

Ohio Department of Administrative Services  
Office of Legal Services  
30 East Broad Street, 40th Floor  
Columbus, Ohio 43215  
Main: (614) 644-1773  
Direct: (614) 995-1766  
Fax: 614.644.8151  
Email: [eric.c.harrell@das.state.oh.us](mailto:eric.c.harrell@das.state.oh.us)

**6.2. Business Associate Mitigation.** In addition, 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 the requirements of this Agreement, and report its mitigation activity back to the agency. Business Associate shall preserve evidence.

**6.3. Coordination.** Business Associate will coordinate with the agency to determine additional, specific actions that will be required of the Business Associate for mitigation of the Breach, which may include notification to the individuals,

entities or other authorities. Notifications, if any, will be made at the direction of the agency.

- 6.4. Incident costs.** Business Associate shall bear all costs associated with the incident. This may include, but not be limited to, costs associated with notifying affected individuals. It also may include the cost of investigation, remediation, and assistance to individuals including services such as a standard level of credit-monitoring such as Debix's standard service or other comparable service available to Ohio agencies under state term schedules.
- 7. Agency Indemnification.** Business Associate hereby indemnifies Agency and agrees to hold Agency harmless from and against any and all losses, expense, damage or injury that Agency may sustain as a result of, or arising out of, Business Associate, or its agent's or subcontractor's, unauthorized use or disclosure of PHI.
- 8. Subcontractor Obligations.** Business Associate shall ensure that all of its subcontractors and agents are bound, in writing, by the same restrictions and obligations contained herein, including but not limited to the obligation to implement reasonable and appropriate safeguards to protect the information, whenever PHI is made accessible to such subcontractors or agents. The Business Associate obtain Agency approval prior to entering into such agreements.
- 9. Access to PHI.** Business Associate shall make all PHI and related information maintained by Business Associate or its agents or subcontractors available as soon as practicable following a request for PHI, but within fifteen (15) days, to the extent necessary to fulfill the following obligations:
- 9.1. Inspection and Copying.** Make the PHI maintained by Associate or its agents or subcontractors in Designated Record Sets available to Agency for inspection and copying to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act.
- 9.2. Accounting.** To account for disclosures of PHI in accordance with the provisions of the Privacy Rule, including, but not limited to 45 CFR § 164.528 and the HITECH Act; and shall make all PHI in its possession available to Agency as soon as practicable following a request for PHI, but within fifteen (15) days, to fulfill Agency's obligation to amend PHI and related information in accordance with 45 CFR § 164.526, and shall, as directed by Agency, incorporate any amendments or related statements into the information held by the Business Associate and any subcontractors or agents.
- 10. Compliance and HHS Access.** The Business Associate shall make available to the agency and to the Secretary of the U.S. Department of Health and Human Services any and all internal practices, documentation, books, and records related to the use and disclosure of PHI received from the agency, or created or received by the Business Associate on behalf of the agency. Such access is for the purpose of determining the agency's compliance with HIPAA, regulations promulgated by the United States Department of Health and Human Services, and any amendment thereto. Any non-compliance by the Business Associate with the terms of this Agreement or the privacy and security regulations shall be a breach of this Agreement if the Business Associate knew of the breach and failed to take

immediate and reasonable steps to cure the non-compliance. The Business Associate agrees that Agency has the right to immediately terminate this Agreement and seek relief, if Agency determines that the Business Associate has violated a material term of the Agreement.

- 11. Ownership and Destruction of Information.** The PHI and any related information created or received from or on behalf of Agency is and shall remain the property of the Agency. The Business Associate agrees that it acquires no title in or rights to the information, including any de-identified information. Upon termination of this Agreement, Business Associate agrees, at the option of Agency, to return or securely destroy all PHI created or received from or on behalf of Agency following 74 FR 19006 Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII. The Business Associate agrees that it will not retain any copies of PHI except as required by law. If PHI is destroyed, the Business Associate agrees to provide Agency with appropriate documentation or certification evidencing such destruction. If return or destruction of all PHI and all copies of PHI is not feasible, the Business Associate agrees to extend the protections of this Agreement to such information for as long as it is maintained and to limit further uses and disclosures to those which make return or destruction infeasible. Termination of this Agreement shall not affect any of its provisions that, by wording or nature, are intended to remain effective and to continue in operation.
- 12. Termination.** Notwithstanding any term or condition in the underlying agreement, the State may terminate the underlying agreement if at any time it determines that the Associate has violated a material term of this Business Associate Agreement. In the alternative, the State may, at its sole discretion, take any action provided in the underlying agreement, may suspend the Agreement, or may allow Associate a reasonable period of time to cure before termination, when such action is determined to be in the State's best interest. Upon suspension of the agreement, the State may, at its sole discretion, require the Associate to comply with the requirements of Paragraph 11, Ownership and Destruction of Information, in the same manner as though the agreement had been terminated. This paragraph shall in no way alter, amend, limit or change the terms and conditions in the underlying agreement as they relate to performance of the underlying agreement, and shall solely relate to violation of the terms of the Business Associate Agreement.
- 13. Survivorship.** The obligations to safeguard the confidentiality, privacy and security of PHI imposed herein shall survive the termination of this Agreement.
- 14. Injunctive Relief.** Notwithstanding any rights or remedies under this Agreement or provided by law, Agency retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of PHI by the Business Associate, any of its subcontractors or agents, or any third party who has received PHI from the Business Associate.
- 15. Binding Effect.** Subject to the limitations on assignment provided elsewhere in this Agreement, the Agreement shall be binding on the parties and their successors, but neither party may assign the Agreement without the prior written consent of the other, which consent shall not be unreasonably withheld. This Agreement will be

binding upon and inure to the benefit of the respective successors and assigns of the State and the Associate.

- 16. Ambiguities, Strict Performance and Priorities.** Any ambiguities in this Agreement shall be resolved in favor of an interpretation that promotes compliance with HIPAA, regulations promulgated thereunder and HITECH. Any conflicts in the security and privacy terms and conditions of this agreement with those in the underlying agreement shall be interpreted to favor of the terms and conditions that promote greater degree of security and privacy. The parties agree that any modifications to those laws shall modify the obligations of the parties hereunder without the need for formal amendment of the Agreement. Any other amendments to this Agreement shall not be effective without the written agreement of both parties. This Agreement will be construed in accordance with the plain meaning of its language and neither for nor against the drafting party. The headings in this Agreement are for convenience only and will not affect the interpretation of any of the Agreement terms and conditions. If at any time either party fails to demand strict performance by the other party of any of the terms of this Agreement, such failure will not be construed as a waiver of any such term, and either party may at any time demand strict and complete performance by the other party.
- 17. Notice.** For any notice under this Agreement to be effective the notice must be made in writing and sent to the address of the appropriate contact provided in the Agreement.
- 18.** Notwithstanding section 6 of this Agreement, any notice to the other party pursuant to this Agreement shall be deemed provided if sent by first class United States mail, postage prepaid, as follows:

To Agency:

To Business Associate:

IN WITNESS WHEREOF, the parties hereto agree to the foregoing,

**[Business Associate Name Here]**

**Ohio Department of  
Administrative Services**

\_\_\_\_\_  
Representative

\_\_\_\_\_  
Representative

\_\_\_\_\_  
Title

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date:

\_\_\_\_\_  
Date:

