

## **HIPAA BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (“BAA”), under the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191 (“HIPAA”), is effective \_\_\_\_\_, 20\_\_, by and between the TRS Pension Trust System, the Texas Public School Retired Employees Group Benefits Program, and the Texas School Employees Uniform Group Health Coverage Program (together, the “System and Programs”), the Teacher Retirement System of Texas, acting in its capacity as trustee of the System and Programs, and \_\_\_\_\_ (“Business Associate”), regarding Business Associate’s obligations as a business associate of the System and Programs for purposes of complying with HIPAA, the HIPAA Rules, and HITECH.

### WITNESSETH

WHEREAS, the System, the Programs, and Business Associate have entered into a contractual agreement effective \_\_\_\_\_, 20\_\_, (the “Agreement”) under which Business Associate contracted to provide certain functions, activities, or services (collectively “Services”) to the System and Programs, and in the continued performance of these Services may access, create, receive, maintain, retain, modify, record, store, transmit, destroy, or otherwise hold, Use, Disclose, or have access to Protected Health Information from or on behalf of the System and Programs;

WHEREAS, the parties agree that this BAA shall be attached to the Agreement and incorporated therein for all purposes as if restated in full;

WHEREAS, this BAA is intended to ensure that Business Associate will establish and implement appropriate safeguards (including certain administrative and security requirements) for the Protected Health Information the Business Associate (and all of its agents, contractors, and Subcontractors that create or receive Protected Health Information in connection with Services to the System and Programs) may access, create, receive, maintain, retain, modify, record, store, transmit, destroy, or otherwise hold, Use, Disclose, or have access to Protected Health Information in connection with Services by Business Associate to the System and Programs; and

WHEREAS, the parties agree that this BAA shall apply to all services provided by the Business Associate to the System and Programs, under the Agreement or any other agreement now existing or hereafter entered into between the System and/or the Programs, on the one hand, and Business Associate, on the other hand;

NOW THEREFORE, in consideration of the parties' continuing obligations under the Agreement, in compliance with HIPAA, the HIPAA Rules, and HITECH, and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, the parties agree to the provisions of this BAA in order to address the statutory obligations imposed upon them and to protect the interests of the parties.

The recitals set forth hereinabove are true and correct in all respects and are incorporated herein by reference fully as if set forth herein.

## I. DEFINITIONS

The following terms used in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclose or Disclosure, Health Care Operations, Minimum Necessary, Notice of Privacy Practices, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Terms used but not otherwise defined in this BAA shall have the same meaning as those terms in the HIPAA Rules.

- A. Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 C.F.R. §160.103, and in reference to the party to this agreement, shall mean \_\_\_\_\_.
- B. Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 C.F.R. §160.103, and in reference to the party to this agreement, shall mean the System, the Programs, and the Teacher Retirement System of Texas, acting in its capacity as trustee of the System and Programs.
- C. HHS. “HHS” shall mean U. S. Department of Health and Human Services.
- D. HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164.
- E. HITECH. “HITECH” shall mean the Health Information Technology for Economic and Clinical Health Act (enacted as part of the American Recovery and Reinvestment Act of 2009), including Sections 164.308, 164.310, 164.312, and 164.316 of Title 45 of the Code of Federal Regulations.
- F. Individual. “Individual” shall have the same meaning as the term “individual” in the HIPAA Rules and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g).
- G. Privacy Rule. “Privacy Rule” shall mean the Standards of Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E, et seq., as amended from time to time.
- H. Programs. “Programs” shall mean the Texas Public School Retired Employees Group Benefits Program (also known as TRS-Care) and the Texas School Employees Uniform Group Health Coverage Program (also known as TRS-ActiveCare).
- I. Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” has in the HIPAA Rules, limited to the information created or received by Business Associate (as well as its agents, contractors, or Subcontractors) from or on behalf of Covered Entity.
- J. Security. “Security” shall have the same meaning as the term “security” at 45 C.F.R. §164.304.

- K. Security Rule. "Security Rule" shall mean those provisions found in 45 C.F.R. Part 164, Subpart C (45 C.F.R. §164.302 - §164.318), as amended from time to time.
- L. System. "System" shall mean the TRS Pension Trust System.

## **II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE**

- A. Business Associate shall comply with HIPAA (including but not limited to the HIPAA Rules), HIPAA regulations, the requirements of HITECH, rules adopted by the Secretary regarding Breaches of Unsecured Protected Health Information, and all applicable state and federal security and privacy laws. In so doing, Business Associate shall adopt privacy and security policies and procedures that are consistent with the requirements of the HIPAA Rules and HITECH, as applicable to Business Associate.
- B. Business Associate shall not Use or Disclose Protected Health Information other than as permitted or required by this BAA or as permitted under law or Required by Law. Subject to Section II. A. immediately above, Business Associate shall follow any written instructions received from Covered Entity with respect to restricting the Uses and Disclosures of Protected Health Information. Business Associate shall ensure that the Protected Health Information is not Used or Disclosed in a manner that would violate the restriction, unless otherwise directed by Covered Entity.
- C. Business Associate shall implement, maintain and use appropriate safeguards (*e.g.*, administrative safeguards, physical safeguards, and technical safeguards) that (i) reasonably and appropriately protect the confidentiality, integrity and availability of Protected Health Information as required by the HIPAA Rules and (ii) comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic Protected Health Information. Business Associate shall prevent Use or Disclosure of Protected Health Information other than as provided for by the HIPAA Rules, Subpart C of 45 C.F.R. Part 164, and this BAA. Business Associate covenants that such safeguards shall include, without limitation, implementing written policies and procedures in compliance with HIPAA, the HIPAA Rules, and HITECH, conducting a security risk assessment, conducting risk assessments concerning possible Breaches, and training its employees who will have access to Protected Health Information with respect to the policies and procedures required by HIPAA, the HIPAA Rules, and HITECH.
- D. Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information by Business Associate (as well as its agents, contractors, or Subcontractors that create or receive Protected Health Information in connection with Services to the System and Programs) that is not provided for by the HIPAA Rules or by this BAA, including Breaches of Unsecured Protected Health Information as required at 45 C.F.R. §164.410, and shall report to Covered Entity any Security Incident of which Business Associate becomes aware.
- E. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of Protected Health Information by Business Associate (as well as by its agents, contractors, or Subcontractors that create or

receive Protected Health Information in connection with Services to the System and Programs) in violation of this BAA or of any Security Incident of which it becomes aware.

- F. Business Associate agrees to ensure that any agency and any agent, contractor, or Subcontractor of Business Associate that accesses, creates, receives, maintains, retains, modifies, records, stores, transmits, destroys, or otherwise holds, Uses, or Discloses Protected Health Information in connection with Services to the System and Programs agrees to the same restrictions, conditions, and requirements that apply through this BAA to Business Associate with respect to Protected Health Information.
- G. In accordance with the HIPAA Rules, Business Associate shall provide reasonable access to Protected Health Information in a Designated Record Set to Covered Entity, or, as directed by Covered Entity to an Individual in order to meet the requirements under 45 C.F.R. §164.524.
- H. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. §164.526 at the request of Covered Entity or an Individual in a reasonable time and manner, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. §164.526.
- I. For purposes of the Secretary determining Covered Entity's compliance with the HIPAA Rules or this BAA, Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the Use and Disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity or to the Secretary (or its agents) in a reasonable time and manner or a time and manner designated by the Covered Entity or the Secretary.
- J. Business Associate shall document and maintain such Disclosures of Protected Health Information and information related to such Disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of Disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528.
- K. At Covered Entity's request, Business Associate shall provide to Covered Entity or an Individual, in a reasonable time and manner, information collected in accordance with subsection J of this section to permit Covered Entity to respond to a request by an Individual for an accounting of Disclosures of Protected Health Information in accordance with 45 C.F.R. §164.528.
- L. When necessary to accommodate an Individual's reasonable requests for confidential communications, Business Associate shall communicate with an Individual regarding his/her Protected Health Information only in the alternative manner or at the alternative location instructed by Covered Entity, unless otherwise directed by Covered Entity.
- M. At Covered Entity's request, Business Associate shall make available Protected Health Information in its possession or under its control in Designated Record Sets for amendment,

and shall incorporate any amendments to Protected Health Information in accordance with the requirements of the HIPAA Rules and any instructions provided by Covered Entity.

- N. If Business Associate accesses, creates, receives, maintains, retains, modifies, records, stores, transmits, destroys, or otherwise holds, Uses, or Discloses Unsecured Protected Health Information, it shall notify Covered Entity without unreasonable delay after a determination has been made that an incident has occurred that requires notification, but in no case later than five (5) business days after the determination in the case of Breaches of electronic Unsecured Protected Health Information relating to the Covered Entity and ten (10) business days after the determination in the case of Breaches of hardcopy Unsecured Protected Health Information belonging to the Covered Entity. In the event of a Breach, Business Associate will provide as much information as is available at the given point in the investigation, as follows: (1) the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired or Disclosed during such Breach; (2) a brief description of what happened, including the date of the Breach and discovery of the Breach; (3) a description of the type of Unsecured Protected Health Information that was involved in the Breach; (4) a description of the investigation into and risk assessment concerning the Breach, mitigation of harm to the Individual(s), and protection against further Breaches; (5) the results of any and all investigations and risk assessments performed by Business Associate related to the Breach; and (6) contact information of the most knowledgeable individual with the Business Associate (or with its agents, contractors, or Subcontractors that create or receive Protected Health Information in connection with Services to the System and Programs) for Covered Entity to contact relating to the Breach and its investigation into and risk assessment concerning the Breach. The Business Associate shall bear all financial costs associated with a Breach arising out of or relating to the performance of, or failure to perform, negligence, willful misconduct or breach of obligations under this BAA by Business Associate and/or its agents, contractors, partners, employees, Subcontractors, consultants, or assignees, except to the extent such Breach is due to the gross negligence or willful misconduct of the Covered Entity. Upon request by Covered Entity, but only upon such request, as to Breaches caused by Business Associate (or by its agents, contractors, or Subcontractors that create or receive Protected Health Information in connection with Services to the System and Programs), Business Associate will communicate with an Individual concerning a Breach that involves the Individual and, when necessary, will communicate with the Department of Health and Human Services and the media. Within ten (10) business days of receiving all the information necessary to make its decision, the Covered Entity will inform the Business Associate of its decision as to whether notification is required and whether it is requesting Business Associate to perform the member notification.
- O. Business Associate represents that if applicable, it has policies and procedures in place designed to detect, prevent and mitigate the risk of identity theft to comply with the Federal Trade Commission's Identity Theft Prevention Red Flags Rule (16 C.F.R. §681.2).
- P. Business Associate shall maintain at its own expense insurance covering all claims, losses, liabilities, judgments, settlements, lawsuits, regulatory actions, fines and other costs or damages arising out of its performance under the Agreement and this BAA, including any negligent or otherwise wrongful acts or omissions by the Business Associate and/or its agents,

contractors, partners, employees, Subcontractors, consultants, or assignees. This includes, but is not limited to: any breach of HIPAA, the HIPAA Rules, HITECH, the Omnibus Final Rule or any other law or regulation governing confidentiality of Protected Health Information.

The policy or policies comprising the above-required insurance coverage shall together provide limits of liability of at least \$10 million in the aggregate. By requiring this insurance, Covered Entity does not represent that coverage and limits will be adequate to indemnify or address the liabilities arising out of a breach of Protected Health Information, and such insurance and limits shall not limit Business Associate's liability under this Agreement.

Upon the Covered Entity's request, the Business Associate shall provide the Covered Entity with a copy of all certificates or verifications of insurance evidencing the existence of the above-required insurance coverage required hereunder.

Failure of Business Associate to obtain and maintain the required insurance is a material breach of this BAA, which may result in termination of the Agreement for cause, at the option of Covered Entity.

Business Associate shall indemnify, protect, defend (with counsel selected by Covered Entity in consultation with the Attorney General that does not have any conflict of interest under applicable law, the public policy of the State of Texas, the Texas Rules of Disciplinary Conduct, or the TRS Code of Ethics for Contractors) and hold harmless Covered Entity, their respective trustees, officers, directors, employees, agents, the System and Programs, and the respective fund of the System and each Program (collectively "Indemnitees") from and against any and all claims, causes of action, liabilities, damages, losses, lawsuits, liens, judgments, or expenses (including attorney fees) of any nature, kind or description, including indemnification for administrative penalties and fines, costs expended to notify participants and/or to prevent or remedy possible identity theft or any other claims related to a Breach ("Indemnified Amounts") incurred by any Indemnitees arising out of or relating to the performance of, or failure to perform, negligence, willful misconduct or breach of obligations under this BAA by Business Associate and/or its agents, partners, employees, Subcontractors, consultants, or assignees, except to the extent such Indemnified Amounts are due to the gross negligence or willful misconduct of any Indemnatee. The provisions of this section shall not be construed to eliminate or reduce any other indemnification or right which Covered Entity has by law.

The duty to indemnify, defend and hold harmless is independent of the duty to insure and continues to apply even in the event insurance coverage required in this BAA or the Agreement is denied, or coverage rights are reserved by any insurance carrier.

To the extent permitted by law, Business Associate's obligation to defend, indemnify and hold harmless any Indemnatee will survive the expiration or termination of the Agreement or this BAA.

- Q. In the event that Business Associate transmits or receives any Covered Electronic Transaction on behalf of Covered Entity, it shall comply with all applicable provisions of the Standards for Electronic Transactions Rule to the extent Required by Law.

- R. Covered Entity and Business Associate recognize and agree that in some instances Business Associate may have compliance obligations as a health care provider under the HIPAA Rules and nothing herein shall prohibit, restrict, or otherwise limit compliance with any such obligations by Business Associate under the HIPAA Rules.
- S. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s).

### **III. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE**

- A. Except as otherwise allowed in this BAA, Business Associate agrees to and may create, receive, Use or Disclose Protected Health Information only to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Agreement to which this BAA is an exhibit, provided that any Use or Disclosure of Protected Health Information would not violate (i) the HIPAA Rules if done by Covered Entity or (ii) the Minimum Necessary standards Required by Law.
- B. Business Associate may Disclose Protected Health Information when such Disclosure is Required by Law.
- C. Business Associate may Use Protected Health Information as Required by Law or to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. §164.502 (j)(1).
- D. Business Associate may Use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
- E. Business Associate is authorized to use Protected Health Information to de-identify the information in accordance with 45 C.F.R. 45 C.F.R. §164.514(a)-(c).

### **IV. OBLIGATIONS OF COVERED ENTITY**

- A. Covered Entity shall notify Business Associate of any limitation(s) in its Notice of Privacy Practices of Covered Entity in accordance with 45 C.F.R. §164.520, to the extent that such limitation(s) affect Business Associate's permitted Use or Disclosure of Protected Health Information.
- B. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to Use or Disclose Protected Health Information, to the extent that such changes affect Business Associate's permitted Use or Disclosure of Protected Health Information.

- C. Covered Entity shall notify Business Associate of any restriction to the Use or Disclosure of Protected Health Information that Covered Entity has agreed to or is required to abide by in accordance with 45 C.F.R. §164.522, to the extent that such restriction affects Business Associate's permitted Use or Disclosure of Protected Health Information.

#### **V. IMPERMISSIBLE REQUESTS BY COVERED ENTITY**

Covered Entity shall not request Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity.

#### **VI. TERM AND TERMINATION**

- A. Term. The term of this BAA shall be effective as of \_\_\_\_\_, 20\_\_\_. Unless terminated for cause, this BAA shall remain in effect during the term of the Agreement, including any extensions, amendments and renewals of the Agreement.
- B. Business Associate shall destroy or return to Covered Entity within ninety (90) days of the termination of the Agreement, all of the Protected Health Information provided by Covered Entity to Business Associate (and to all of its agents, contractors, and Subcontractors that create or receive Protected Health Information in connection with Services to the System and Programs), or created or received by Business Associate (and all of its agents, contractors, and Subcontractors that create or receive Protected Health Information in connection with Services to the System and Programs) on behalf of Covered Entity. Upon such destruction or return, Business Associate shall provide a written certification to the Covered Entity that includes all of the following: (i) a statement confirming that all of the Protected Health Information described immediately above has been destroyed or returned to the Covered Entity; (ii) a detailed description of the Protected Health Information that was destroyed or returned to the Covered Entity; and (iii) a statement that describes the mechanism by which all of the Protected Health Information described immediately above was destroyed or returned to the Covered Entity.
- C. Upon the termination of the Agreement, this BAA shall terminate when the Business Associate (i) destroys or returns to Covered Entity all of the Protected Health Information described immediately above and (ii) provides the above described written certification to the Covered Entity.
- D. Termination for Cause. Upon Covered Entity's knowledge of a material breach of this BAA, HIPAA, the HIPAA Rules, HIPAA regulations and/or HITECH by Business Associate (or its agents, employees, contractors, and Subcontractors), Covered Entity shall either:
1. on the one hand, provide an opportunity for Business Associate to cure the breach or end the violation, or, on the other hand, terminate this BAA if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or
  2. immediately terminate this BAA if Business Associate has breached a material term of this BAA and cure is not possible; or

3. if neither termination nor cure is feasible, report the violation to the Secretary. The parties agree that if Covered Entity terminates this BAA pursuant to this section, it shall also terminate all provisions of the Agreement that relate to Business Associate's Use or Disclosure of Protected Health Information and Covered Entity shall have the discretion to terminate the Agreement in its entirety and pursue all remedies available under the Agreement.

## **VII. MISCELLANEOUS**

- A. A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.
- B. Covered Entity and Business Associate agree to take such action as is necessary to amend this BAA from time to time as required for Covered Entity to comply with the provisions of HIPAA, the HIPAA Rules, HITECH, and any other applicable law.
- C. The terms of the HIPAA Rules may be expressly amended from time to time by HHS, or as a result of interpretations by HHS, a court, or another regulatory agency with authority over the parties. In such an event, the parties will work together in good faith to determine the impact on the parties' obligations and whether the specific event requires the need to amend this BAA.
- D. Modification of the terms of this BAA shall not be effective or binding upon the parties unless and until such modification is committed to writing and executed by the parties hereto.
- E. Any ambiguity in this BAA shall be interpreted and resolved to permit compliance with HIPAA, the HIPAA Rules, and HITECH.
- F. In the event of a conflict or inconsistency between the terms of this BAA and the Agreement, the provisions of this BAA shall prevail.
- G. In the event of an inconsistency between the terms of this BAA and the mandatory terms of the HIPAA Rules, the mandatory terms of the HIPAA Rules shall prevail. Where the terms of this BAA are different from those included in the HIPAA Rules but the terms of the HIPAA Rules are permissive, the terms of this BAA shall control.
- H. Business Associate is solely responsible for all decisions made by Business Associate, its agents, contractors, and Subcontractors that access, create, receive, maintain, retain, modify, record, store, transmit, destroy, or otherwise hold, Use, or Disclose Protected Health Information in connection with Services to the System and Programs, regarding the safeguarding of Protected Health Information. Notwithstanding, this section does not relieve any agent, contractor or Subcontractor of any responsibility or liability in connection with their respective actions and omissions.

- I. Should any provision of this BAA be found unenforceable, it shall be deemed severable and the balance of the BAA shall continue in full force and effect as if the unenforceable provision had never been made a part hereof.
- J. This BAA does not create or confer any rights or remedies onto third parties.
- K. This BAA, including such portions as are incorporated by reference herein, constitutes the entire BAA by, between and among the parties, and such parties acknowledge by their signature hereto that they do not rely upon any representations or undertakings by any person or party, past or future, not expressly set forth in writing herein.
- L. This BAA shall be binding upon the parties hereto, and their respective legal representatives, trustees, receivers, successors and permitted assigns.
- M. To the extent not preempted by federal law, this BAA and the rights and obligations of the parties hereunder shall in all respects be governed by, and construed in accordance with the laws of the State of Texas, including all matters of construction, validity and performance.
- N. All notices and communications required or permitted to be given hereunder shall be sent by certified or regular mail, addressed to the other parties at their respective address as shown on the signature page, or at such other address as such party shall from time to time designate in writing to the other parties, and shall be effective from the date of mailing.

THE REMAINDER OF THIS PAGE HAS  
INTENTIONALLY BEEN LEFT BLANK

O. The provisions of Sections II.A., II. B., II. C., II. D., II. E., II. G., II. H., II. I., II. J., II. K., II. N., II. P., II. S., and VI. shall survive termination of this BAA.

**IN WITNESS WHEREOF**, the parties have executed this Business Associate Agreement on the date indicated below.

\_\_\_\_\_  
  
By: \_\_\_\_\_  
Printed Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Date: \_\_\_\_\_

**The TRS Pension Trust System, the Texas Public School Retired Employees Group Benefits Program, and the Texas School Employees Uniform Group Health Coverage Program**

By: \_\_\_\_\_  
Brian K. Guthrie  
  
Title: Executive Director of the Teacher Retirement System of Texas, acting as trustee of the TRS Pension Trust System, the Texas Public School Retired Employees Group Benefits Program, and the Texas School Employees Uniform Group Health Coverage Program  
  
Date: \_\_\_\_\_

**Teacher Retirement System of Texas**

By: \_\_\_\_\_  
Brian K. Guthrie  
  
Title: Executive Director  
  
Date: \_\_\_\_\_