



**Re: Business Associate Agreement for HIPAA Compliance**

Dear Policyholder;

Because you engage in the management and distribution of patients' protected health information, you are a "Covered Entity", as defined in the Health Insurance Portability and Accountability Act, commonly known as "HIPAA". You are therefore required to have a Business Associate Agreement (BAA) with Healthcare Providers Insurance Exchange, your professional medical liability insurance provider, which is a Business Associate of yours, as defined in HIPAA.

To assist you in complying with HIPAA, we have posted on our web site our BBA signed by me as President and CEO. This agreement satisfies the HIPAA requirement that your Business Associates, in this case HPIX, provide you with a written assurance that they will abide by the HIPAA guidelines.

**All you need to do is download the BAA and print it out. You should file the printed BAA with the other documents relating to your HPIX coverage or in your files relating to HIPAA compliance.**

The enclosed BAA does not modify or supersede any of the terms and conditions of your insurance policy with HPIX, nor does it satisfy the requirement that you obtain a BAA from each of your other Business Associates. You should speak with your other Business Associates directly regarding this aspect of HIPAA compliance.

You may have already received a copy of this BAA with your policy issuance or renewal documents. In that case, you need not print out a second copy of the BAA. If you have any questions about the BAA, please call D. Scott Jones, CHC; Senior Vice President, Claims, Risk Management and Corporate Compliance at 717.237.5503.

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas Gaudiosi".

Thomas Gaudiosi  
President and CEO

## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“BAA”) is made effective as provided in Section 8(a) of this agreement by Healthcare Providers Insurance Exchange (“Business Associate”) for the benefit of an insured (“Covered Entity”) to which an insurance policy has been issued by Business Associate.

### RECITALS

A. Business Associate is providing professional liability insurance coverage to Covered Entity pursuant to an insurance policy and its attachments, as such may be amended and renewed from time to time (together, the “Insurance Policy”). Pursuant to the Insurance Policy, Covered Entity has agreed to reporting requirements that may involve the disclosure of “PHI”, as hereinafter defined, to Business Associate.

B. The purpose of this BAA is to satisfy the standards and requirements of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”) and the HIPAA Regulations, including, but not limited to, Title 45, Section 164.504(e) of the Code of Federal Regulations (“CFR”), as the same may be amended from time to time, that Business Associate provide Covered Entity, as a covered entity under HIPAA, with “satisfactory assurances” that Business Associate will deal with PHI that it receives from Covered Entity pursuant to the Insurance Policy in a manner that is compliant with Covered Entity’s responsibilities under HIPAA.

In consideration of the foregoing, Business Associate agrees as follows:

#### 1. **Definitions.** For purposes of this BAA, the following terms have the following definitions:

- (a) *Individual.* “Individual” shall have the same meaning as the term “individual” in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- (b) *Privacy Rule.* “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.
- (c) *PHI.* “PHI” shall have the same meaning as the term “protected health information” in 45 CFR 164.501, but is limited to the PHI received by Business Associate from Covered Entity.
- (d) *Required By Law.* “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR 164.501.
- (e) *Secretary.* “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.
- (f) *Security Incident.* “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.
- (g) *Designated Record Set.* “Designated Record Set” shall have the same meaning as the term “Designated Record Set” in 45 CFR 165.501, but is limited to the medical records information received by Business Associate from Covered Entity.

## **2. Obligations and Activities of Business Associate as to PHI.**

- (a) Business Associate agrees to not use or further disclose PHI other than as permitted or required by the Insurance Policy, this BAA or as required by law.
- (b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for in the Insurance Policy and this BAA.
- (c) Business Associate agrees to mitigate, to the extent reasonably 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 BAA.
- (d) Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this BAA.
- (e) Business Associate agrees to require that any agent, including a subcontractor, to whom it provides PHI on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such information.
- (f) Business Associate agrees to provide access during normal business hours, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as reasonably directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524.
- (g) Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity.
- (h) Business Associate agrees to make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to Covered Entity, or at the request of Covered Entity to the Secretary, in a time and manner designated by Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule. Business Associate agrees to document such disclosures of PHI 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 PHI in accordance with 45 CFR 164.528.
- (i) Business Associate agrees to provide to Covered Entity during normal business hours, in the time and manner reasonably designated by Covered Entity, information to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528, to the extent that, pursuant to the Insurance Policy, Business Associate makes any such disclosures.

**3. Permitted Uses and Disclosures of PHI by Business Associate.** Except as otherwise permitted in this BAA, Business Associate may use or disclose PHI only to perform the functions, activities or services for, or on behalf of, Covered Entity as set forth in the Insurance Policy, a use which Covered Entity represents would not violate: (i) the Privacy Rule if done by Covered Entity; or (ii) the "Minimum Necessary" policy and procedures of Covered Entity. In addition,

- (a) Except as otherwise limited in this BAA or the Insurance Policy, Business Associate may use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
- (b) Except as otherwise limited in this BAA or the Insurance Policy, Business Associate may disclose PHI: (i) for the proper management and administration of Business Associate; (ii) if required by law; or (iii) if Business Associate obtains reasonable assurances from the

person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to such person, and such person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

#### ***4. Obligations of Covered Entity to Inform Business Associate of Privacy Practices and Individual Restrictions.***

Covered Entity shall provide Business Associate with the following:

- (a) Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- (b) Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes affect Business Associate's permitted or required uses and disclosures.
- (c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

#### ***5. Permissible Requests by Covered Entity***

Except as specifically provided in the Insurance Policy or in this BAA, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

#### ***6. Security Standards Requirements***

The parties acknowledge that the Security Standards require certain additional satisfactory assurances from Business Associate to Covered Entity. Business Associate agrees to the following additional obligations:

- (a) Business Associate will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity as required by the Security Standards;
- (b) Business Associate will require that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- (c) Business Associate will report to Covered Entity any Security Incident of which it becomes aware;
- (d) Business Associate authorizes termination of the Insurance Policy if Covered Entity determines that Business Associate has violated a material term of this BAA.

## **7. Obligations of Business Associate under the American Recovery and Reinvestment Act of 2009 and the Red Flags Rule.**

- (a) *Notice of Breach of Unsecured Information.* Effective not later than thirty (30) days after the Secretary publishes implementing regulations, Business Associate will establish effective systems to monitor and detect a Breach of Unsecured Protected Health Information accessed, maintained, retained, modified, stored, destroyed or otherwise held or used in Unsecured form by Business Associate, whether the Unsecured Protected Health Information is in paper or electronic form. Business Associate will provide to the Chief Privacy Officer of Covered Entity, or to such other individual designated by Covered Entity in writing, written notice of a breach involving Covered Entity's PHI within three (3) business days after the first day the breach is known to Business Associate, including for this purpose any employee, officer or other agent of the Business Associate (other than the individual committing the breach). The notice will include the identification of each individual whose Unsecured Protected Health Information was, or is reasonably believed to have been, subject to the breach. Without limiting Covered Entity's rights or Business Associate's responsibilities in the event of a breach involving Covered Entity's PHI: (i) Business Associate will promptly reimburse Covered Entity for all costs and expenses incurred by Covered Entity in providing required Breach Notification to individuals or to regulatory agencies and (ii) Covered Entity may treat the breach as a material breach of the Insurance Policy.
- (b) *Identity Theft Detection Program.* Business Entity shall have an Identity Theft Detection Program in place that is compliant, and is consistent with Covered Entity's compliance, with the Federal Trade Commission Final Rule on Identity Theft Red Flags as it relates to any information provided by Covered Entity to Business Associate and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003 (the "Red Flags Rule") published at 16 CFR Part 681, as may be subsequently modified or amended. Unless otherwise requested by Covered Entity, in the event of discovery by Business Associate of a Red Fla, within the meaning of the Red Flags Rule, that relates to any information provided by Covered Entity to Business Associate, Business Entity will report the Red Flag immediately to Covered Entity and comply with such further steps, at Business Entity's expense, as are requested by Covered Entity as are reasonable and appropriate under the Red Flags Rule, such as consumer notification and taking further prevention and mitigation steps.

## **8. Term and Termination**

- (a) *Term.* This BAA shall be effective as of as of the effective date of the Insurance Policy 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) *Termination for Cause.* Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

- (1) Provide an opportunity for Business Associate to cure the breach or end the violation in a manner reasonably proposed by Covered Entity. In either event, Covered Entity may terminate the Insurance Policy if Business Associate does not cure the breach or end the violation within the time specified or agreed to;
  - (2) Notwithstanding the foregoing Section (b) (1), Covered Entity may immediately terminate the Insurance Policy if Business Associate has breached a material term of this BAA and Covered Entity reasonably determines that cure is not possible;
  - (3) Notwithstanding the foregoing Section (b) (1) or (2), if Covered Entity reasonably determines that neither cure, as specified in Section (b) (1) above, nor termination, as specified in Section (b) (2) above, is feasible, Covered Entity shall report the violation to the Secretary.
- (c) *Effect of Termination.* Business Associate has represented and warranted to Covered Entity, in writing, that it is infeasible for Business Associate to return or destroy, upon termination of the Insurance Policy for any reason, all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity. Based on that representation, Covered Entity has agreed that, upon termination of the Insurance Policy for any reason, Business Associate may retain one archive copy of such PHI as needed for Business Associate's internal management purposes, provided Business Associate extends the protections of this BAA to all such PHI and limits further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

## **9. DISCLAIMER**

COVERED ENTITY MAKES NO WARRANTY OR REPRESENTATION THAT COMPLIANCE BY BUSINESS ASSOCIATE WITH THIS BAA OR THE PRIVACY RULE WILL BE ADEQUATE OR SATISFACTORY FOR BUSINESS ASSOCIATE'S OWN PURPOSES. BUSINESS ASSOCIATE IS SOLELY RESPONSIBLE FOR ALL DECISIONS MADE BY BUSINESS ASSOCIATE REGARDING THE SAFEGUARDING OF PHI.

## **10. Miscellaneous**

- (a) *Regulatory References.* A reference in this BAA to a section in the Privacy Rule means the section as in effect or as amended, and for which compliance is required.
- (b) *Amendment.* Business Associate agrees to take such action as is necessary to amend this BAA from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and HIPAA. Business Associate further agrees that, notwithstanding the terms of this BAA, it will do all things necessary for it to comply with the requirements of the Privacy Rule and HIPAA, as may be amended from time to time.
- (c) *Survival.* The rights and obligations of Covered Entity and Business Associate under Section 8(c),(1) and (2) of this BAA shall survive the termination of the Insurance Policy and this BAA.

- (d) *Interpretation.* Any ambiguity in this BAA shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.
- (e) *Notices.* All notices and other communications required or permitted pursuant to this BAA shall be in writing and delivered: by registered or certified mail, return receipt requested; by a nationally recognized overnight carrier; or by hand delivery. Notices to Business Associate shall be addressed to: Healthcare Providers Insurance Exchange, Attention President, 30 South 17<sup>th</sup> Street, 11<sup>th</sup> Floor, Philadelphia, PA 19103-4196. Notices to Covered Entity shall be addressed to its principal place of business as shown on the Insurance Policy.
- (f) *No Third Party Beneficiary.* The provisions and covenants set forth in this BAA are intended solely for the benefit of Covered Entity and Business Associate. Neither Covered Entity nor Business Associate intends to create or establish any third party beneficiary status or right (or the equivalent thereof) in any third party, and no such third party shall have any right to enforce or enjoy any benefit created or established by the provisions and covenants in this BAA.
- (g) *Binding Effect.* This BAA shall be binding upon, and shall inure to the benefit of, Covered Entity and Business Associate and their respective successors and permitted assigns.
- (h) *Entire Agreement.* This BAA contains all the agreements and understandings between Covered Entity and Business Associate with respect to the subject matter hereof. No agreement or other understanding in any way modifying the terms hereof will be binding unless made in writing as a modification or amendment to this BAA and signed by Covered Entity and Business Associate.
- (i) *Governing Law, Jurisdiction and Venue.* This BAA shall be governed by, and interpreted in accordance with, the internal laws of the Commonwealth of Pennsylvania, without giving effect to its conflict of law provisions. Any controversy or claim arising out of or related to this BAA shall be brought solely and exclusively in a court located in Pennsylvania, provided, however, that either Covered Entity or Business Associate may enforce any judgment rendered by such court in any court of competent jurisdiction. Covered Entity and Business Associate hereby consent, and waive any challenge or objection, to personal jurisdiction and venue in Pennsylvania.
- (j) *No Assignment.* The rights and obligations under this BAA may not be assigned either by Covered Entity or Business Associate without the consent of the other.
- (k) *Headings.* The Section headings of this BAA are for convenience only and shall not affect the interpretation of this BAA.

IN WITNESS WHEREOF, Business Associate has duly executed this BAA effective as stated above.

Health Care Providers Insurance Exchange



Thomas Gaudiosi  
President and Chief Executive Officer

