

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (this "*Agreement*") is by and between You, the Covered Entity ("*Covered Entity*"), and Paubox, Inc. ("*Business Associate*"). This BAA is effective as of the date You electronically indicate Your acceptance of this BAA ("Effective Date").

RECITALS:

BY ACCEPTING THIS AGREEMENT OR USING THE SERVICES, AS DEFINED IN OUR TERMS OF SERVICE, YOU AGREE TO THESE TERMS AND CONDITIONS. IF YOU ARE ENTERING INTO THIS AGREEMENT AS AN INDIVIDUAL, THE TERM "COVERED ENTITY" REFERS TO YOU. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERM "COVERED ENTITY" SHALL REFER TO SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE PAUBOX SERVICES FOR THE STORAGE OR TRANSMISSION OF PROTECTED HEALTH INFORMATION ("PHI").

WHEREAS, Business Associate has entered into an agreement with Covered Entity for the purposes of performing certain services for Covered Entity (the terms and conditions of such agreement between the parties hereinafter referred to as the "*Terms of Service*");

WHEREAS, pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (the "*Act*") and the "Health Information Technology for Economic and Clinical Health Act," part of the "American Recovery and Reinvestment Act of 2009" ("*HITECH Act*"), the Department of Health and Human Services ("*HHS*") has promulgated regulations at 45 C.F.R. Parts 160-64, including regulations implementing certain privacy requirements (the "*Privacy Rule*"), certain security requirements regarding electronic media ("*Security Rule*") and certain breach notification requirements ("*Breach Notification Rule*"), each as amended from time to time (the Act, HITECH Act, the Privacy Rule, the Security Rule and the Breach Notification Rule referred to collectively herein as "*HIPAA*");

WHEREAS, Business Associate may receive, maintain, retain, record, store, transmit, hold, use and/or disclose Protected Health Information (as defined below) in conjunction with the services being provided under the Terms of Service, thus necessitating a written agreement that meets applicable requirements of the Privacy Rule and the Security Rule, and making advisable certain additional agreements regarding HIPAA; and

WHEREAS, Business Associate and Covered Entity desire to satisfy the foregoing Privacy Rule and Security Rule requirements through this Agreement, and

otherwise to address related matters regarding HIPAA on the terms and conditions set forth herein.

NOW THEREFORE, in consideration of the mutual agreements and undertakings of the parties, and for other good and valuable consideration the sufficiency of which is hereby acknowledged, the parties, intending to be legally bound, hereby agree as follows:

1. **Definitions:**

The following terms shall have the following meaning when used in this Agreement:

- a. *“Breach”* shall have the same meaning as the term “breach” in 45 C.F.R. § 164.402.
- b. *“Designated Record Set”* shall have the same meaning as the term “designated record set” in 45 C.F.R. § 164.501.
- c. *“Electronic Protected Health Information”* shall mean Protected Health Information that is “electronic protected health information” as defined in 45 C.F.R. § 160.103.
- d. *“Individual”* shall have the same meaning as the term “individual” in 45 C.F.R. §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. §164.502(g).
- e. *“Protected Health Information”* shall have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, except limited to the information received from Covered Entity, or created, maintained or received on behalf of Covered Entity.
- f. *“Unsecured Protected Health Information”* shall mean Protected Health Information that is “unsecured protected health information” as defined in 45 C.F.R. § 164.402.
- g. *“Required By Law”* shall have the same meaning as the term “required by law” in 45 C.F.R. § 164.103.
- h. *“Secretary”* shall mean the Secretary of HHS or the designee of the Secretary of HHS.
- i. *“Subcontractor”* shall have the same meaning as the term “subcontractor” in 45 C.F.R. §160.103, except limited to any such individual or entity who creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate.

Any capitalized term not specifically defined herein shall have the same meaning as is set forth in 45 C.F.R. Parts 160 and 164, where applicable. The terms “use,” “disclose” and “discovery,” or derivations thereof, although not capitalized, shall also have the same meanings set forth in HIPAA.

2. **Obligations and Activities of Business Associate:**

- a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.
- b. Business Associate agrees use appropriate safeguards and comply, where applicable, with Subpart C of 45 C.F.R. Part 164 with respect to Electronic Protected Health Information, to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- c. Business Associate agrees to report to the Covered Entity any use or disclosure of Protected Health Information not provided for by this Agreement, including, without limitation, Breaches of Unsecured Protected Health Information as required at 45 C.F.R. 164.410, and any Security Incident of which it becomes aware. The parties acknowledge and agree that this Section 2(c) constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but unsuccessful Security Incidents for which no additional notice to Covered Entity shall be required. Unsuccessful Security Incidents shall include, but not be limited to, pings and other broadcast attacks on Business Associate’s firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as such incidents do not result, to the extent Business Associate is aware, in unauthorized access, use or disclosure of Electronic Protected Health Information.
- d. In accordance with 45 C.F.R. 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, Business Associate agrees to ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate agree in writing to the same restrictions, conditions, and requirements that apply to Business Associate under this Agreement with respect to such Protected Health Information.
- e. Business Associate agrees to make available Protected Health Information in a Designated Record Set to Covered Entity as necessary to satisfy Covered Entity’s obligations under 45 C.F.R. § 164.524.
- f. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 C.F.R. § 164.526.

- g. Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528.
- h. To the extent that Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 C.F.R. Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligations.
- i. Business Associate agrees to make its internal practices, books, and records available to the Secretary for purposes of determining compliance with HIPAA.

3. **Permitted Uses and Disclosures by Business Associate:**

- a. Business Associate may only use or disclose Protected Health Information as necessary to perform services for Covered Entity. In addition, Business Associate is authorized to use Protected Health Information to de-identify the Protected Health Information in accordance with 45 C.F.R. 164.514(a)-(c).
- b. Business Associate may use or disclose Protected Health Information as Required By Law.
- c. Business Associate agrees to make uses and disclosures and requests for Protected Health Information consistent with Covered Entity's minimum necessary policies and procedures.
- d. Business Associate may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific uses and disclosures set forth in subsections (e), (f) and (g), below.
- e. Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- f. Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as Required By Law or for the purposes for which it was disclosed to the person, and the person notified Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

- g. Business Associate may provide Data Aggregation services relating to the Health Care Operations of Covered Entity.

4. **Obligations of Covered Entity:**

- a. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 C.F.R. 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
- b. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
- c. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of Protected Health Information that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.
- d. Except with respect to uses and disclosures by Business Associate of Protected Health Information under Sections 3(e), 3(f) and 3(g), above, Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity

5. **Term and Termination:**

- a. Term. The Term of this Agreement shall commence as of the Effective Date and shall terminate upon the termination of the Terms of Service or on the date Covered Entity terminates this Agreement for cause as authorized in subsection (b) of this Section 5, whichever is sooner.
- b. Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity upon written notice to Business Associate if Covered Entity determines Business Associate has violated a material term of this Agreement and Business Associate has not cured the breach or ended the violation within thirty (30) days of Covered Entity providing written notice thereof to Business Associate.
- c. Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate shall:

(i) Retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(ii) Return to Covered Entity or Covered Entity's designee (to the extent permitted by HIPAA), or, if agreed to by Covered Entity, destroy the remaining Protected Health Information that the Business Associate still maintains in any form;

(iii) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic Protected Health Information to prevent use or disclosure of the Protected Health Information, other than as provided for in this Section, for as long as Business Associate retains Protected Health Information;

(iv) Not use or disclose Protected Health Information retained by Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out at Section 3 (e) and (f), above, which applied prior to termination; and

(v) Return to Covered Entity, or, if agreed to by Covered Entity, destroy Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

d. Survival. The obligations of Business Associate under this Section 5 shall survive the termination of this Agreement.

6. **Miscellaneous:**

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule, the Security Rule, or to another provision of HIPAA means the provision as in effect or as amended.

b. Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the Covered Entity to comply with the requirements of the HIPAA and any other applicable law.

c. Interpretation. Any ambiguity in this Agreement shall be resolved to permit compliance with HIPAA.

d. Governing Law and Disputes. The construction, interpretation and performance of this Agreement and all transactions under this Agreement shall be governed and enforced pursuant to the laws of the State of California, without giving effect to its conflicts of laws provisions, except to the extent California law is preempted by any provision of federal law,

including HIPAA. The Parties agree that all disputes arising out of or relating to this Agreement will be subject to mandatory binding arbitration under the rules of Judicial Administration and Arbitration Services (“JAMS”) in effect at the time of submission, as modified by this Section 6(d). The arbitration will be heard and determined by a single arbitrator selected by mutual agreement of the Parties, or, failing agreement within thirty (30) days following the date of receipt by the respondent of the claim, by JAMS. Such arbitration will take place in San Francisco, CA. The arbitration award so given will be a final and binding determination of the dispute, and will be fully enforceable in any court of competent jurisdiction. Except in a proceeding to enforce the results of the arbitration or as otherwise required by law, neither Party nor any arbitrator may disclose the existence, content or results of any arbitration hereunder without the prior written agreement of both Parties.

- e. No Third Party Beneficiary. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assigns of the parties, any rights, remedies, obligations, or liabilities whatsoever.
- f. Controlling Provisions. In the event that it is impossible to comply with both the Terms of Service and this Agreement, the provisions of this Agreement shall control with respect to those provisions of each agreement that expressly conflict. This Agreement shall supersede and replace any prior business associate agreements between the parties, with respect to any actions of Business Associate after the Effective Date.
- g. Effect. This Agreement shall be binding upon, and shall inure to the benefit of, the parties hereto and their respective successors, assigns, heirs, executors, administrators and other legal representatives.
- h. Severability. In the event any provision of this Agreement is rendered invalid or unenforceable under any new or existing law or regulation, or declared null and void by any court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect if it reasonably can be given effect.
- i. Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original.
- j. Notices. Any notice, consent, request or other communication required or permitted under this Agreement shall be in writing and shall be deemed to have been duly given if delivered personally, by overnight courier or, in the case of notices to Covered Entity, by email, addressed as set forth below. Notice that is

sent by overnight courier shall be deemed given one (1) business day after it is dispatched, provided that receipt is acknowledged.

If to Covered Entity: via email, to the Covered Entity's currently registered email address (as may be updated by the Covered Entity from time to time)

If to Business Associate:

Paubox, Inc.
5 Third Street, Suite 324
San Francisco, CA 94103
Attention: Privacy Officer

BY CLICKING "I ACCEPT", YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THE COVERED ENTITY UNDER THIS AGREEMENT AND ACCEPT ALL TERMS AND CONDITIONS SET FORTH HEREIN.