JOTFORM HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement (“HIPAA BAA”) is made between **Jotform, Inc.**, (“Jotform”) and **{YourCompanyName}** (“Covered Entity” or “Customer”) as an agreement to the Jotform Terms of Use (the “Terms of Use”). This HIPAA BAA is effective as of **{AgreementDate}** (“Effective Date”), which is the date Customer indicated its acceptance of this HIPAA BAA electronically. This HIPAA BAA was electronically signed by **{YourFullName}**, **{YourRole}** on behalf of Customer on the Effective Date.

In accordance with this HIPAA BAA, Customer may disclose to Jotform certain "Protected Health Information" subject to the Health Insurance Portability and Accountability Act of 1996, as codified at 42 U.S.C. Section 1320d-6 and 1320d-9 (“HIPAA”) and any current and future regulations promulgated thereunder, including, without limitation, the federal privacy regulations contained in 45 C.F.R. Parts 160 and 164 Subparts A and E (“Privacy Rules”), the federal security standards contained in 45 C.F.R. Part 160 and 164 Subparts A and C (“Security Rules”), and the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) contained in Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009 (“ARRA”) (all are collectively referred to herein as the “The Regulations”).

Jotform and Customer hereby agree to the terms and conditions of this HIPAA BAA in compliance with the “The Regulations”.

1. Definitions

1.1. The terms of this HIPAA BAA are incorporated herein by reference as part of the Terms of Use to comply with the “The Regulations”.

1.2. Required by law shall have the same meaning as in the term “required by law” in 45 CFR § 164.103.

1.3. “Security Rule” shall mean the Security Standards for the protection of Electronic Protected Health Information, located at 45 CFR Part 160 and Subparts A and C of Part 164

1.4. “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.

1.5. Unless otherwise specified, all terms used in this HIPAA BAA have the meaning set forth in the Privacy Rules and Security Rules.

1.6. “Form Hosting Services” shall mean the building of forms to collect user data including PHI data that will be stored by Jotform.

2. Business Associate Obligations

2.1. **Permitted Uses and Disclosures**. Jotform shall not, and shall ensure that its directors, officers, admin users, employees, contractors do not, use or disclose Protected Health Information ("PHI") created, received, maintained, or transmitted for the customer in any manner that would violate HIPAA. Jotform acknowledges and agrees that it will not use or disclose PHI other than as permitted or required by this HIPAA BAA or as required by law. Except as otherwise limited in this HIPAA BAA, Jotform may use or disclose PHI to perform functions, activities, for the sole purpose of the proper management and administration of Form Hosting Services or services for (or on behalf of) the customer as specified in the Agreement, provided that such use or disclosure would not violate the HIPAA Privacy Rule if done by customer.

2.2. **Use/Disclosure for Administrative Activities**. Notwithstanding Section 2.1, Jotform may use and/or disclose PHI for management and administrative activities of Jotform or to comply with the legal responsibilities of Jotform; provided, however, that with respect to any such disclosure: (i) the disclosure is required by law; or (ii) Jotform obtains reasonable assurances from the third party that receives the PHI that the third party will treat the PHI confidentially and will only use or further disclose the PHI in a manner consistent with the purposes that the PHI was provided by Jotform, and contact support any breach of the confidentiality of the PHI to Jotform.

2.3. **Use of PHI for Data Aggregation**. Except as otherwise limited in this HIPAA BAA, Jotform may use PHI to provide Data Aggregation services to Customer consistent with 45 C.F.R. §164.504(e)(2)(i)(B).

2.4. **Safeguards**. Jotform will implement appropriate safeguards which includes Data Encryption and Encryption In-Transit services and, with respect to Electronic PHI, comply with the applicable provisions of 45 C.F.R Part 164, Subpart C, to prevent any Use or Disclosure of PHI other than as provided for by this HIPAA BAA.

2.5. **Subcontractors of Jotform.** Jotform acknowledges and agrees to enter into written contracts with any agent or independent contractor that creates, receives, maintains, or transmits PHI on behalf of the Jotform with regards to services provided by Jotform pursuant to the Agreement (collectively, "Subcontractors"). Such contracts shall obligate Subcontractor to abide by substantially the same terms and conditions as are required of Jotform and agree to implement reasonable and appropriate safeguards to protect PHI under this HIPAA BAA. Jotform utilizes a small list of sub processors for storage of customer data. See Jotform Subprocessors.

2.6. **Restrictions**. Jotform acknowledges and agrees to comply with any requests for restrictions on certain disclosures of PHI to which Customer has agreed in accordance with 45 C.F.R. § 164.522 and of which Jotform has been notified by Customer.

2.7. **HIPAA Enabled Account Usage**. Customer acknowledges and agrees that PHI shall only be managed or transferred using the Customer's HIPAA Enabled Account. Use of Non-HIPAA Enabled Account with the Business Associate for the transmission of PHI is strictly prohibited.

2.7.1. **Forms**. Customer acknowledges and agrees to only copy forms containing PHI to other HIPAA Enabled Accounts. While building forms, Customer acknowledges and agrees to label PHI fields to grant permission for Jotform in order to maintain additional measures required for PHI protection.

2.7.2. **Data Export**. Customer acknowledges and agrees that Jotform shall not be responsible for PHI after It is exported from Jotform HIPAA Enabled Account and It shall be Customer's responsibility to use and protect exported PHI according to The Regulations. This covers all data export services provided by Jotform.

2.7.3. **Data Sharing**. Customer acknowledges and agrees that PHI shared via Jotform by HIPAA Enabled Account shall abide by Jotform Terms of Service and The Regulations. It will be Customer's sole responsibility after it is shared or transferred. Also, Customer complies that it is Customer's sole responsibility to protect data in further circumstances that indicates The Regulations. This covers all data-sharing services provided by Jotform.

2.7.4. **Third Party Integrations**. Customer acknowledges and agrees to only use Third Party Integrations if;

a) Customer has a BAA or related agreements in place with the Third Party Service Provider consistent under The Regulations, or;
b) Third Party Service Provider publicly announces HIPAA compliance in all the services provided, or;
c) Jotform announces HIPAA Compliant Integration with Third Party Service.

2.8. **Performance of Covered Entity's Obligations**. To the extent Jotform has agreed to carry out one or more of Customer's obligations under 45 C.F.R. Part 164, Subpart E, Jotform shall comply with the requirements of Subpart E that apply to Customer in the performance of such obligations. The parties agree and acknowledge that Business Associate has not agreed to carry out any of Covered Entity's obligations under 45 C.F.R. Part 164, Subpart E.

2.9. **Access and Amendment**. Jotform shall notify the Customer of receipt of a request received by Jotform for access to, or amendment of, PHI. The Customer shall be responsible for responding or objecting to such requests.

2.9.1. **Access**. Upon request, Jotform acknowledges and agrees to furnish Customer with copies of the PHI maintained by Jotform in a Designated Record Set in the time and manner designated by Customer to enable Customer to respond to an individual request for access to PHI under 45 C.F.R. § 164.524.

2.9.2. **Amendment**. Upon request and instruction from Customer, Jotform shall make available PHI for amendment and incorporate any amendments to such PHI in accordance with 45 C.F.R. §164.526 and related laws and regulations.

2.10. **Accounting**. Jotform acknowledges and agrees to document disclosures of PHI as would be required for Customer to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528 and if required by and upon the effective date of, Section 13405(c) of the HITECH Act and related regulatory guidance; and provide to Customer information collected in accordance with this Section. In the event an individual delivers the initial request for an accounting directly to Jotform, Jotform shall forward such request to Customer.

2.11. **Security Obligations.** Jotform shall implement the administrative, physical, and technical safeguards set forth in 45 C.F.R. §§ 164.308, 164.310, and 164.312 that reasonably and appropriately protect the confidentiality, integrity, and availability of any Electronic PHI that Jotform creates, receives, maintains, or transmits on behalf of Customer, and, in accordance with 45 C.F.R. § 164.316, implement and maintain reasonable and appropriate policies and procedures to enable Jotform to comply with the requirements set forth in Sections 164.308, 164.310, and 164.312.

2.12. **Access by Secretary of U.S. Department of Health and Human Services**. Jotform agrees to allow the Secretary of the U.S. Department of Health and Human Services (the "Secretary") access to its books, records, and internal practices with respect to the disclosure of PHI for the purposes of determining the Customer's or Jotform's compliance with HIPAA.

3. **Notification Obligations**

3.1. **Unauthorized Use or Disclosure of PHI**. Jotform shall report to Customer in writing, within ten business days, any use or disclosure of PHI not provided for by this HIPAA BAA of which Jotform becomes aware.

3.2. **Security Incident.** Jotform shall report to Customer in writing, within ten business days, any Security Incident affecting Electronic PHI of Customer of which Jotform becomes aware. The Parties agree that this Section satisfies any notice requirements by Jotform of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Customer shall be required. For purposes of this HIPAA BAA, "Unsuccessful Security Incidents" include: (a) "pings" on an information system firewall; (b) port scans; (c) attempts to log on to an information system or enter a database with an invalid password or user name; (d) denial-of-service attacks that do not result in a server being taken offline; or (e) malware (e.g., a worm or virus) that does not result in unauthorized access, use, disclosure, modification, or destruction of Electronic PHI.

3.3. **Breach of Unsecured PHI**. Jotform will notify Customer of any Breach of Unsecured PHI in accordance with 45 C.F.R. §164.410. The notice required by this Section will be written in plain language and will include, to the extent possible or available, the following:

> 3.3.1. The identification of each individual whose Unsecured PHI has been, or is reasonably believed by Jotform to have been, accessed, acquired, used, or disclosed during the Breach;

3.3.2. A brief description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;

3.3.3. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3.3.4. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

3.3.5. A brief description of what is being done to investigate the Breach, mitigate the harm, and protect against future Breaches; and

3.3.6. Contact procedures for Individuals to ask questions or learn additional information which shall include a toll-free number, an e-mail address, Web site, or postal address, if Customer specifically requests Jotform to establish contact procedures.

4. **Covered Entity's Obligations**

4.1. **Notice of Privacy Practices.** Customer shall, upon request, provide Jotform with its current notice of privacy practices adopted in accordance with HIPAA.

4.2. **Limitations in Notice of Privacy Practices.** Customer shall notify Jotform of any limitations in the notice of privacy practices of Customer under 45 C.F.R. §164.520, to the extent that such limitation may affect Jotform's use or disclosure of PHI.

4.3. **Restrictions or Changes in Authorization**. Customer shall not agree to any non-mandatory restrictions on the use or disclosure of Protected Health Information if such restriction could affect Jotform's permitted or required uses and disclosures of PHI hereunder except upon Jotform's express, written consent. Customer shall notify Jotform of any changes, revocations or restrictions of the use or disclosure of PHI if such changes, revocations or restrictions affect Jotform's permitted or required uses and disclosures of PHI hereunder including, without limitation, any revocation of any authorization for the use or disclosure of PHI.

4.4. **Requests for Use and Disclosure.** Customer shall not request that Jotform collect, access, use, maintain or disclose PHI, or act in any manner, contrary to or in violation or breach of the Regulations or this HIPAA BAA.

4.5. **Appropriate Use**. Jotform is a tool for securely collecting complex information using customizable forms. Jotform is not an electronic health record or other medical record system and should not be used to maintain a Designated Record Set or relied upon directly to provide patient care. Information collected via Jotform must be transferred into an appropriate system of record (for example, an electronic health record) in accordance with appropriate processes to assure confidentiality, accuracy and availability before being used for patient care.

4.6. **Communications Made Outside of Jotform, Inc.** Customer acknowledges and agrees that texting and other communications of protected health information that Customer request Jotform to relay outside of the Jotform pose heightened privacy and security risks. Customer further acknowledges and agrees that it is Customer's sole responsibility to determine, as part of its HIPAA Risk Analysis, whether to prohibit or permit such communications and, to the extent such communications are permitted, to implement appropriate safeguards (including policies, procedures and training of all authorized users) to manage these risks to a reasonable and appropriate level consistent with HIPAA.

5. **Termination**

5.1. **Termination upon Material Breach**. Upon Customer's knowledge of a material breach of this HIPAA BAA by Jotform, Customer shall notify Jotform of such breach in reasonable detail and provide an opportunity for Jotform to cure the breach or violation, or if cure is not possible, Customer may immediately terminate this HIPAA BAA.

5.2. **Return or Destruction of PHI.** Upon termination of this HIPAA BAA, Jotform will return to Customer all PHI received from Customer or created or received by Jotform on behalf of Customer which Jotform maintains in any form or format, and Jotform will not maintain or keep in any form or format any portion of such PHI. Alternatively, Jotform may destroy all such PHI and provide written documentation of such destruction.

5.3. **Alternative Measures**. If the return or destruction of PHI is not feasible upon termination of the HIPAA BAA, then Jotform acknowledges and agrees that it shall extend its obligations under this HIPAA BAA to protect the PHI and limit the use or disclosure of PHI to those purposes that make the return or destruction of PHI infeasible.

6. **Third Party Beneficiaries**

6.1. **No Third-Party Beneficiary Rights**. Nothing express or implied in this HIPAA BAA is intended or shall be interpreted to create or confer any rights, remedies, obligations, or liabilities whatsoever in any third party.

7. **Miscellaneous**

7.1. **Survival**. Customer and Business Associate's respective rights and obligations under this HIPAA BAA shall survive the termination of the Agreement.

7.2. **Interpretation.** Any ambiguity in the Jotform Terms shall be resolved to permit Customer to comply with HIPAA and the Privacy Rule.

{YourCompanyName}		JOTFORM, INC.	
BY		BY	
NAME	{YourFullName}	NAME	
TITLE	{YourRole}	TITLE	
ADDRESS	{YourCompanyAddress}	ADDRESS	4 Embarcadero Center, Suite 780, San Francisco CA 94111
DATE	{AgreementDate}	DATE	{AgreementDate}
EMAIL	{YourEmailAddress}		

4 Embarcadero Center, Suite 780, San Francisco CA 94111