HIPAA BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum ("BAA") is made between Cognito, LLC., a South Carolina corporation ("Cognito Forms") and {OrganizationLegalName} ("Covered Entity" or "{Organization}") as an addendum to the Cognito Forms Terms of Service (the "Terms of Service"). This BAA is effective as of {AgreementDate} ("Effective Date"), which is the date {Organization} indicated its acceptance of this BAA electronically. This BAA was electronically signed by {RepresentativeName}, {RepresentativeTitle} on behalf of {Organization} on the Effective Date.

{if OrganizationType = "Business Associate"}{Organization} is a Business Associate of Covered Entities and Cognito Forms is Business Associate Subcontractor. {Organization} will be responsible for Covered Entity obligations in this BAA and/or ensure the Covered Entities they work with fulfill these obligations. Specifically, {Organization} will ensure that all applicable Notices of Privacy Practice permit use of Cognito Forms by {Organization}, that no Covered Entity has agreed to any additional restriction which would prohibit use of Cognito Forms by {Organization}, and that all Covered Entities have obtained any authorization or consent necessary for use of Cognito Forms by {Organization}.

{end if}In connection with this BAA, {Organization} may disclose to Cognito Forms 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 "Regulations").

Cognito Forms and {Organization} hereby agree to the terms and conditions of this BAA in compliance with the Regulations.

1. Scope and Definitions

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

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

2. Business Associate Obligations

2.1. **Permitted Uses and Disclosures.** Cognito Forms shall not, and shall ensure that its directors, officers, employees, contractors and agents do not, use or disclose Protected Health Information ("PHI") created, received, maintained, or transmitted for the {Organization} in any manner that would violate HIPAA. Cognito Forms agrees that it will not use or disclose PHI other than as permitted or required by this BAA or as required by law. Except as otherwise limited in this BAA, Cognito Forms may use or disclose PHI to perform functions, activities, or services for (or on behalf of) the {Organization} as specified in the Agreement, provided that such use or disclosure would not violate the HIPAA Privacy Rule if done by {Organization}.

2.2. **Use/Disclosure for Administrative Activities.** Notwithstanding Section 2.1, Cognito Forms may use and/or disclose PHI for management and administrative activities of Cognito Forms or to comply with the legal responsibilities of Cognito Forms; provided, however, that with respect to any such disclosure: (i) the disclosure is required by law; or (ii) Cognito Forms 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 Cognito Forms, and promptly report any breach of the confidentiality of the PHI to Cognito Forms.

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

2.4. **Safeguards.** Cognito Forms will implement appropriate safeguards 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 BAA.

2.5. **Subcontractors of Cognito Forms.** Cognito Forms agrees to enter into written contracts with any agent or independent contractor that creates, receives, maintains, or transmits PHI on behalf of the Cognito Forms with regard to services provided by Cognito Forms pursuant to the Agreement (collectively, "Subcontractors"). Such contracts shall obligate Subcontractor to abide by substantially the same terms and conditions as are required of Cognito Forms under this BAA.

2.5.1. **Microsoft Azure.** Cognito Forms uses Microsoft Azure to provide highly available, highly scalable, and highly secure hosting for both services and data. Cognito Forms has entered into a BAA with Microsoft covering all aspects of Cognito Forms' hosting via Microsoft Azure.

2.5.2. **Mailgun.** Cognito Forms uses Mailgun, a transactional email service, to send email notifications and confirmations for all HIPAA BAA organizations. Mailgun provides a BAA for HIPAA-compliant email transmissions through their servers. However, per HIPAA guidelines, individual consent is always required to send emails containing PHI to patients due to the inherently unsecure nature of email delivery. When building forms, mark PHI fields as protected to ensure they will not be included in email messages and/or request consent before sending PHI via email through Cognito Forms.

2.5.3. **Microsoft Power Automate.** Cognito Forms integrates with Microsoft Power Automate to enable integration with hundreds of other cloud services. This integration requires a separate BAA directly with Microsoft, as {Organization} controls the information and processing once it is transmitted securely by Cognito Forms to Power Automate. Not all services Power Automate connects to are HIPAA compliant. Microsoft Power Automate should be used as an alternative to Zapier, as Zapier does not offer a BAA covering their services.

2.5.4. **JSON Post.** JSON webhooks allow Cognito Forms to communicate with a third-party system (or internally developed application) to securely transmit data. This integration requires custom development and hosting, along with relevant security measures to be HIPAA compliant.

2.5.5. **SharePoint.** Cognito Forms integrates with Microsoft SharePoint to share data in lists. This integration requires a separate BAA directly with Microsoft when using SharePoint Online. SharePoint on-premise is potentially HIPAA compliant, but {Organization} shall be responsible for maintaining compliance.

2.5.6. **Square.** Cognito Forms integrates with Square for secure payment processing. This integration requires a separate BAA directly with Square, as {Organization} controls how payments are processed and how Square uses this information. Alternative payment processors (including PayPal and Stripe)

should be avoided, as they do not offer BAAs covering their services.

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

2.7. **Performance of Covered Entity's Obligations.** To the extent Cognito Forms has agreed to carry out one or more of {Organization}'s obligations under 45 C.F.R. Part 164, Subpart E, Cognito Forms shall comply with the requirements of Subpart E that apply to {Organization} 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.

2.8. **Access and Amendment.** Cognito Forms shall notify the {Organization} of receipt of a request received by Cognito Forms for access to, or amendment of, PHI. The {Organization} shall be responsible for responding or objecting to such requests.

2.8.1. **Access**. Upon request, Cognito Forms agrees to furnish {Organization} with copies of the PHI maintained by Cognito Forms in a Designated Record Set in the time and manner designated by {Organization} to enable {Organization} to respond to an individual request for access to PHI under 45 C.F.R. § 164.524.

2.8.2. **Amendment.** Upon request and instruction from {Organization}, Cognito Forms shall make available PHI for amendment and incorporate any amendments to such PHI in accordance with 45 C.F.R. § 164.526.

2.9. **Accounting.** Cognito Forms agrees to document disclosures of PHI as would be required for {Organization} 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 {Organization} information collected in accordance with this Section. In the event an individual delivers the initial request for an accounting directly to Cognito Forms, Cognito Forms shall forward such request to {Organization}.

2.10. **Security Obligations.** Cognito Forms 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 Cognito Forms creates, receives, maintains, or transmits on behalf of {Organization}, and, in accordance with 45 C.F.R. § 164.316, implement and maintain reasonable and appropriate policies and procedures to enable Cognito Forms to comply with the requirements set forth in Sections 164.308, 164.310, and 164.312.

2.11. **Access by Secretary of U.S. Department of Health and Human Services.** Cognito Forms 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 {Organization}'s or Cognito Forms' compliance with HIPAA.

3. Notification Obligations

3.1. **Unauthorized Use or Disclosure of PHI.** Cognito Forms shall report to {Organization} in writing, within ten business days, any use or disclosure of PHI not provided for by this BAA of which Cognito Forms becomes aware.

3.2. **Security Incident.** Cognito Forms shall report to {Organization} in writing, within ten business days, any Security Incident affecting Electronic PHI of {Organization} of which Cognito Forms becomes aware. The

Parties agree that this Section satisfies any notice requirements by Cognito Forms of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to {Organization} shall be required. For purposes of this 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.** Cognito Forms will notify {Organization} 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 Cognito Forms 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 {Organization} specifically requests Cognito Forms to establish contact procedures.

4. Covered Entity's Obligations

4.1. **Notice of Privacy Practices.** {Organization} shall, upon request, provide Cognito Forms with its current notice of privacy practices adopted in accordance with HIPAA.

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

4.3. **Restrictions or Changes in Authorization.** {Organization} shall not agree to any non-mandatory restrictions on the use or disclosure of Protected Health Information if such restriction could affect Cognito Forms' permitted or required uses and disclosures of PHI hereunder except upon Cognito Forms' express, written consent. {Organization} shall notify Cognito Forms of any changes, revocations or restrictions of the use or disclosure of PHI if such changes, revocations or restrictions affect Cognito Forms' 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.** {Organization} shall not request that Cognito Forms collect, access, use, maintain or disclose PHI, or act in any manner, contrary to or in violation or breach of the Regulations or this BAA.

4.5. **Subscription Plan**. This BAA may only be entered into by organizations on the Enterprise plan. {Organization} must remain on the Enterprise plan (or any equivalent successor plan) and may not downgrade or otherwise change the subscription plan while this BAA is in effect.

4.6. **Appropriate Use.** Cognito Forms is a tool for securely collecting complex information using customizable forms. Cognito Forms 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 Cognito Forms 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.

5. Termination

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

5.2. **Return or Destruction of PHI.** Upon termination of this BAA, Cognito Forms will return to {Organization} all PHI received from {Organization} or created or received by Cognito Forms on behalf of {Organization} which Cognito Forms maintains in any form or format, and Cognito Forms will not maintain or keep in any form or format any portion of such PHI. Alternatively, Cognito Forms 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 BAA, then Cognito Forms agrees that it shall extend its obligations under this 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 BAA is intended or shall be interpreted to create or confer any rights, remedies, obligations, or liabilities whatsoever in any third party.

Agreement Date: {AgreementDate}

{OrganizationLegalName}

By:
{Signature}
{RepresentativeName}
{RepresentativeTitle}

Cognito, LLC

By:

Jamie Thomas
Co-founder