

BUSINESS ASSOCIATE AGREEMENT

This **BUSINESS ASSOCIATE AGREEMENT** (this "**BA Agreement**") is made effective on _____, 201_ (the "**Effective Date**"), by and between **THINK SMART GROUP INC.**, a California corporation ("**TSI**"), and _____ ("**End User**"). TSI and End User may be referred to individually as a "**Party**" and collectively as the "**Parties**". Capitalized terms used in this BA Agreement without definition shall have the respective meanings assigned to such terms by End User License Agreement between the Parties effective on the Effective Date (the "**EULA**"), or the Administrative Simplification section of the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act and their implementing regulations as amended from time to time (collectively, "**HIPAA**").

RECITALS

WHEREAS, TSI receives Protected Health Information from or on behalf of End User pursuant to the EULA ("**PHI**"); and

WHEREAS, the Parties desire to amend the EULA to add the Business Associate Agreement provisions set forth in this BA Agreement in order for the Parties to comply with HIPAA.

NOW THEREFORE, in consideration of the mutual premises and covenants contained herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

AGREEMENT

I. OBLIGATIONS OF TSI

Section 1.1. Use and Disclosure of PHI. TSI may use and disclose PHI as permitted or required under this BA Agreement or as Required by Law, but shall not otherwise use or disclose PHI. TSI shall not use or disclose PHI received from End User in any manner that would constitute a violation of HIPAA if so used or disclosed by End User (except as set forth in Sections 1.1(b), (c), (d) and (e) of this BA Agreement). To the extent TSI carries out any of End User's obligations under the HIPAA Privacy Rule, TSI shall comply with the requirements of the HIPAA Privacy Rule that apply to End User in the performance of such obligations. Without limiting the generality of the foregoing, TSI is permitted to use or disclose PHI as set forth below:

(a) TSI and its Subcontractors may use and disclose PHI to carry out TSI's duties and obligations and exercise their rights under the EULA.

(b) TSI and its Subcontractors may use PHI internally for TSI's or the Subcontractor's proper management and administrative services or to carry out their legal responsibilities;

(c) TSI and its Subcontractors may disclose PHI to a third party for TSI's or the Subcontractor's proper management and administration, provided that the disclosure is Required by Law or TSI or the Subcontractor, as applicable, obtains reasonable assurances from the third party to whom the PHI is to be disclosed that the third party will (1) protect the confidentiality of the PHI, (2) only use or further disclose the PHI as Required by Law or for the purpose for which the PHI was disclosed to the third party and (3) notify, as applicable, TSI or the Subcontractor of any instances of which the person is aware in which the confidentiality of the PHI has been breached;

(d) TSI and its Subcontractors may use PHI to provide Data Aggregation services; and

(e) TSI and its Subcontractors may use PHI to create de-identified health information in accordance with the HIPAA de-identification requirements. Without limiting any other rights of TSI under the EULA, TSI may use, create, sell, disclose to third parties and otherwise exploit de-identified health information for any purposes not

prohibited by law. For the avoidance of doubt, the second sentence of this Section 1.1(e) shall survive the expiration or earlier termination of the EULA or this BA Agreement.

Section 1.2. Safeguards. TSI shall use reasonable and appropriate safeguards to prevent the use or disclosure of PHI except as otherwise permitted or required by this BA Agreement. In addition, TSI shall implement Administrative Safeguards, Physical Safeguards and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of PHI transmitted or maintained in Electronic Media (“**EPHI**”) that it creates, receives, maintains or transmits on behalf of End User. TSI shall comply with the HIPAA Security Rule with respect to EPHI.

Section 1.3. Minimum Necessary Standard. To the extent required by the “minimum necessary” requirements of HIPAA, TSI shall only request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure.

Section 1.4. Mitigation. TSI shall take reasonable steps to mitigate, to the extent practicable, any harmful effect (that is known to TSI) of a use or disclosure of PHI by TSI in violation of this BA Agreement.

Section 1.5. Subcontractors. TSI shall enter into a written agreement meeting the requirements of 45 C.F.R. §§ 164.504(e) and 164.314(a)(2) with each Subcontractor that creates, receives, maintains or transmits PHI on behalf of TSI. TSI shall ensure that the written agreement with each Subcontractor obligates the Subcontractor to comply with restrictions and conditions that are at least as restrictive as the restrictions and conditions that apply to TSI under this BA Agreement.

Section 1.6. Reporting Requirements.

(a) If TSI becomes aware of a use or disclosure of PHI in violation of this BA Agreement by TSI or by a third party to which TSI disclosed PHI, TSI shall report any such use or disclosure to End User without unreasonable delay.

(b) TSI shall report any Security Incident involving EPHI of which it becomes aware in the following manner: (a) any actual, successful Security Incident will be reported to End User in writing without unreasonable delay, and (b) any attempted, unsuccessful Security Incident of which TSI becomes aware will be reported to End User orally or in writing on a reasonable basis, as requested by End User. If the HIPAA Security Rule is amended to remove the requirement to report any unsuccessful Security Incidents, the requirement hereunder to report such unsuccessful Security Incidents will no longer apply as of the effective date of the amendment.

(c) TSI shall, following the discovery of a Breach of Unsecured PHI, notify End User of the Breach in accordance with 45 C.F.R. § 164.410 without unreasonable delay and in no case later than sixty (60) days after discovery of the Breach.

Section 1.7. Access to Information. TSI shall make available PHI in the software and/or products identified in the EULA to End User in accordance with the EULA for so long as TSI maintains the PHI in a Designated Record Set. If TSI receives a request for access to PHI directly from an Individual, TSI shall forward such request to End User within ten (10) business days. End User shall have the sole responsibility for determining whether to approve a request for access to PHI and to provide such access to the Individual.

Section 1.8. Availability of PHI for Amendment. TSI shall provide PHI in the [Software] to End User for amendment, and incorporate any such amendments in the PHI (for so long as TSI maintains such information in the Designated Record Set), in accordance with this BA Agreement and as required by 45 C.F.R. § 164.526. If TSI receives a request for amendment to PHI directly from an Individual, TSI shall forward such request to End User within ten (10) business days. End User shall have the sole responsibility for determining whether to approve an amendment to PHI and to make such amendment.

Section 1.9. Accounting of Disclosures. Within thirty (30) business days of written notice by End User to TSI that it has received a request for an accounting of disclosures of PHI (other than disclosures to which an exception to the accounting requirement applies), TSI shall make available to End User such information as is in TSI's possession and is required for End User to make the accounting required by 45 C.F.R. § 164.528. If TSI receives a request for an accounting directly from an Individual, TSI shall forward such request to End User within ten (10) business days. End User shall have the sole responsibility for providing an accounting to the Individual.

Section 1.10. Availability of Books and Records. Following reasonable advance written notice, TSI shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by TSI on behalf of, End User available to the Secretary for purposes of determining End User's compliance with HIPAA.

II. OBLIGATIONS OF END USER

Section 2.1. Permissible Requests. End User shall not request TSI to use or disclose PHI in any manner that would not be permissible under HIPAA if done by End User.

Section 2.2. Minimum Necessary Information. When End User discloses PHI to TSI, End User shall provide the minimum amount of PHI necessary for the accomplishment of End User's purpose.

Section 2.3. Appropriate Use of PHI. End User and its employees, representatives, consultants, contractors and agents shall not submit any Protected Health Information to TSI (A) outside of the Software, including but not limited to submissions to any online forum made available by TSI or its Subcontractors to their customers, email transmissions, and submissions through any support website, portal, or online help desk or similar service made available by TSI or its Subcontractors outside of **[the Software]**; or (B) directly to any third party involved in the provision of an online forum, email, support website, online help desk or other service described in (A), above.

Section 2.4. Permissions; Restrictions. End User warrants that it has obtained and will obtain any consent, authorization and/or other legal permission required under HIPAA and other applicable law for the disclosure of PHI to TSI. End User shall notify TSI of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect TSI's use or disclosure of PHI. End User shall not agree to any restriction on the use or disclosure of PHI under 45 C.F.R. § 164.522 that restricts TSI's use or disclosure of PHI under the EULA and this BA Agreement) unless such restriction is Required By Law or TSI grants its written consent.

Section 2.5. Notice of Privacy Practices. Except as Required By Law, with TSI's consent or as set forth in this BA Agreement, End User shall not include any limitation in End User's notice of privacy practices that limits TSI's use or disclosure of PHI under the EULA or this BA Agreement.

III. TERMINATION OF THE EULA AND THIS BA AGREEMENT

Section 3.1. BA Agreement Term. This BA Agreement shall continue in full force and effect for so long as TSI maintains any PHI.

Section 3.2. Termination Upon Breach of this BA Agreement. Any other provision of the EULA notwithstanding, the EULA and this BA Agreement may be terminated by either Party (the "**Non-Breaching Party**") upon ninety (90) days written notice to the other Party (the "**Breaching Party**") in the event that the Breaching Party materially breaches this BA Agreement in any material respect and such breach is not cured within such ninety (90) day period. Any determination of whether a material breach has been cured shall be made by TSI in its sole discretion.

Section 3.3. Return or Destruction of PHI upon Termination. Upon termination of the EULA, TSI shall return or destroy all PHI received from End User or created or received by TSI on behalf of End User and which TSI still maintains as PHI. Notwithstanding the foregoing, to the extent that TSI determines, in its sole discretion, that it is not feasible to return or destroy such PHI, this BA Agreement (including, without limitation, Section 1.1(e) of this BA Agreement) shall survive termination of the EULA and this BA Agreement and such PHI shall be used or disclosed solely for such purpose or purposes which prevented the return or destruction of such PHI.

IV. MISCELLANEOUS PROVISIONS

Section 4.1. Applicability. This BA Agreement relates to PHI that TSI or TSI's Subcontractors receive pursuant to the EULA.

Section 4.2. HIPAA Amendments. The Parties acknowledge and agree that the Health Information Technology for Economic and Clinical Health Act and its implementing regulations impose requirements with respect to privacy, security and breach notification applicable to Business Associates (collectively, the "**HITECH BA Provisions**"). The HITECH BA Provisions and any other future amendments to HIPAA affecting Business Associate Agreements are hereby incorporated by reference into this BA Agreement as if set forth in this BA Agreement in their entirety, effective on the later of the Effective Date or such subsequent date as may be specified by HIPAA.

Section 4.3. Regulatory References. A reference in this BA Agreement to a section in HIPAA means the section as it may be amended from time-to-time.

Section 4.4. Relationship of the Parties. Neither the EULA nor this BA Agreement create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties and the status of the Parties shall be independent parties to a contractual arrangement. Neither Party shall have the authority to bind the other Party by contract or otherwise.

Section 4.5. Entire Agreement. The EULA and this BA Agreement constitute the entire agreement between the Parties as to their subject matter, and supersede all previous and contemporaneous agreements, proposals or representations, written or oral, concerning such subject matter. Except as otherwise set forth therein, no modification, amendment, or waiver of any provision of this BA Agreement shall be effective unless in writing and signed by the Party against whom the modification, amendment, or waiver is to be asserted.

Section 4.6. Waiver. No failure or delay by either Party in exercising any right under this Agreement shall constitute a waiver of that right. Other than as expressly stated therein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a Party at law or in equity.

Section 4.7. Counterparts. This BA Agreement may be executed in one or more counterparts, which may be delivered by fax or other electronic transmission, including email, each of which shall be deemed an original and which taken together shall form one legal instrument.

IN WITNESS WHEREOF, each Party has caused its duly authorized representative to execute this BA Agreement as of the Effective Date.

THINK SMART GROUP INC.

Think Smart Group Inc.



Rob Ross
President
Think Smart Group Inc.