BUSINESS ASSOCIATE AGREEMENT

This **Business Associate Agreement** (the "BAA") is entered into by and between the Client, Sponsor, TPA or other party identified on the "Order Form" (as defined below) (such other party hereinafter referred to as the "Covered Entity") and **HealthJoy, LLC** (the "Business Associate"), and sets forth the parties' agreement for the privacy and security requirements under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including 45 C.F.R. Parts 160 and 164 ("Privacy Rule") and the Security Standards set forth at 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subpart A and Subpart C (the "Security Rule"), as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") and included in the American Recovery and Reinvestment Act of 2009 ("ARRA"), the Gramm Leach Bliley Act ("GLBA"), and the regulations promulgated from time to time under each of those acts. In the event the other Party is not a "Covered Entity" but will share PHI, NPI, or NPPI (as each are defined below) with HealthJoy, such other Party shall be considered a Covered Entity for purposes of the defined term in this BAA.

The parties agree that the terms of this BAA shall fully replace any previous Business Associate Addendum or Business Associate terms and conditions. The parties also agree that this BAA shall be subject to and incorporated into the applicable Order Form and the "HealthJoy Terms and Conditions" (or other named written agreement) by and between the parties that governs Covered Entity's and its Member's use of the HealthJoy App programs and related services (collectively, the "Terms and Conditions").

This BAA shall be effective ("BAA Effective Date") as the date of the Client Program Order Form, the Client Agreement, Program Agreement, Client Terms and Conditions, Third-Party License Agreement, Partnership, or other ordering document (hereinafter referred to as the "Order Form").

Capitalized terms not otherwise defined in this BAA or in the Terms and Conditions shall have the same meaning as outlined in regulations promulgated under HIPAA, GLBA or ARRA, as may be amended from time to time.

Business Associate provides the following "Services" to Covered Entity: Outreach and engagement services to eligible members on behalf of employer groups separately engaged by Covered Entity and Business Associate.

The parties agree as follows:

1. **Business Associate Services.** The Services provided by Business Associate for Covered Entity may involve the use and disclosure of individually identifiable health information, deemed protected health information or "PHI" under HIPAA and non-public personal information ("NPPI") under the Gramm Leach Bliley Act and applicable state law and regulations; PHI and NPPI shall be referred to collectively as "Non-Public Information" or "NPI." Except as otherwise provided herein, the Business Associate may make all uses of NPI necessary to perform the Services and its obligations under this BAA and the Terms and Conditions.

2. **Additional Business Associate Activities.** Except as otherwise provided in this BAA, Business Associate may use and disclose the NPI in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of the Business Associate, provided that such uses are permitted under state and federal laws and would be permissible if performed by Covered Entity.

3. **Business Associate Obligations for Privacy and Security of NPI.**

   Business Associate agrees to the following:

   3.1 **Use and Disclosure of NPI.** The Business Associate shall not use or further disclose the NPI other than as permitted under this BAA, the Terms and Conditions, HIPAA, GLBA, ARRA, and their respective implementing regulations, each as amended from time to time. Business Associate agrees that (i) any such disclosures it makes will be required by law or to perform its obligations hereunder, including, without limitation, in the Terms and Conditions; and (ii) the Business Associate will obtain a written agreement from any such person or entity to whom the NPI will be disclosed that the NPI will be held confidentially and will not be further used or disclosed except as required by laws or for the purpose for which it was lawfully disclosed to such person or entity, and that such person or entity will notify the Business Associate of any instances of which it is aware in which the confidentiality of the NPI has been breached.

   3.2 **Safeguards.** Business Associate shall (i) use appropriate safeguards to prevent the use or disclosure of NPI other than as provided for in this BAA, and (ii) have administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of NPI that it creates, receives, maintains, or transmits on behalf of Covered Entity. Upon

written request from Covered Entity, Business Associate shall provide Covered Entity with a copy of its written information privacy and security programs.

3.3 **Policies and Procedures**. Business Associate shall adopt and comply with policies and procedures that are in accordance with the HIPAA, ARRA, and GLBA requirements that apply to Business Associate's operations and the Services provided under the Terms and Conditions, including, without limitations, maintaining the confidentiality and integrity of any information received, maintained, or transmitted by or on behalf of Covered Entity. Upon written request from Covered Entity, Business Associate shall provide a copy of such policies and procedures.

3.4 **Incident Reporting.**

3.4.1 "Breach" means the unauthorized acquisition, access, use or disclosure of NPI which compromises the security or privacy of such information.

3.4.2 "Unsecured NPI" means NPI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary from time to time.

3.4.3 Business Associate will report to Covered Entity any security incident of which it becomes aware involving use or disclosure of NPI not permitted by this BAA. Business Associate will report to Covered Entity any instance of unauthorized use or disclosure pursuant to Section 3.5 below. Notwithstanding the foregoing, the parties acknowledge that unsuccessful security incidents that occur within the normal course of business will not be reported pursuant to this Agreement; such unsuccessful security incidents include, but are not limited to, port scans or "pings", and unsuccessful log-on attempts, broadcast attacks on Business Associate's firewall, denials of service or any combination thereof if such incidents are detected and neutralized by Business Associate's anti-virus and other defensive software and not allowed past Business Associate's firewall.

3.4.4 Covered Entity will be responsible to provide notification to individuals whose NPI has been disclosed, as well as the Secretary of the U.S. Department of Health and Human Services (or such other federal or state agencies with appropriate oversight authority) (the "Secretary") and the media, as required by Section 13402 of the HITECH Act.

3.4.5 Business Associate agrees to establish procedures to assist the Covered Entity to investigate the Breach, mitigate losses, and protect against any future Breaches, and to provide a description of these procedures and the specific findings of the investigation to Covered Entity in the time and manner reasonably requested by Covered Entity. Business Associate agrees to bear its costs for the efforts outlined in this Section 3.4.4 in the event the Breach was caused by Business Associate; if the Breach was not caused by the Business Associate or its subcontractors, then the Covered Entity agrees to reimburse Business Associate for its expenses in performing its obligations in this BAA in response to such Breach.

3.5 **Notification of Breach**. Business Associate shall report any Breach of Unsecured PHI to Covered Entity following discovery and without unreasonable delay (ideally within 10 days after discovery). Notice of Breach shall include, at minimum: (i) the identification of each individual whose NPI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during the Breach; (ii) the date of the Breach, if known; (iii) the scope of the Breach; and (iv) a description of the Business Associate's response to the Breach. Upon reasonable written request from Covered Entity, Business Associate shall provide Covered Entity with information related to the Breach and will cooperate with Covered Entity in any required notifications. Business Associate agrees to bear its costs for the efforts outlined in this Section 3.5 in the event the Breach was caused by Business Associate; if the Breach was not caused by the Business Associate or its subcontractors, then the Covered Entity agrees to reimburse Business Associate for its expenses in performing its obligations in this Section 3.5.

3.6 **Government Programs**. To the extent that Business Associate provides services to Covered Entity relating to individuals enrolled in state or federal programs (e.g., Medicare, Medicaid), Business Associate shall comply with any additional restrictions or requirements related to the use, disclosure, maintenance, and protection of NPI of individuals enrolled in such programs through Covered Entity. For the NPI of Medicare enrollees, Business Associate shall report privacy and security incidents

or Breaches without unreasonable delay to Covered Entity and include the information required under Sections 3.4 and 3.5 of this BAA.

3.7 **Subcontractors.** Business Associate shall require any agent or subcontractor to whom Business Associate provides NPI to agree in writing to (i) implement reasonable and appropriate safeguards to protect the NPI and (ii) comply with the same restrictions and conditions on NPI as required by this BAA. Upon written request from Covered Entity, Business Associate shall provide a copy of any such agreement.

3.8 **Minimum Necessary.** Business Associate shall request, use, or disclose only the minimum amount of NPI necessary to accomplish the purpose of the request, use or disclosure.

3.9 **Remuneration of NPI.** Business Associate shall not directly or indirectly receive remuneration in exchange for any NPI as prohibited by 42 U.S.C. §17935(d) and any regulations promulgated thereunder.

4. **Requested Restrictions on Use of NPI.** Covered Entity will notify Business Associate of any restrictions on the use or disclosure of NPI that have been received from individuals and agreed to by Covered Entity. Business Associate will endeavor to comply with such restrictions.

5. **Prohibition on Use or Disclosure of PHI for Reproductive Health Care.** In compliance with recent changes to the HIPAA Privacy Rule, Covered Entity and Business Associate agree that neither party shall use or disclose any individual's PHI for the purpose of conducting a criminal, civil, or administrative investigation into or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances, or for the identification of any person for the purpose of conducting such investigation or imposing such liability.

5.1 **Presumption of Lawfulness.** Both parties agree that reproductive health care provided by a person other than the parties is presumed lawful under the circumstances in which it was provided, unless the Covered Entity or Business Associate has actual knowledge that the care was unlawful or receives factual information from the requesting party demonstrating a substantial basis that the care was not lawful. Neither party shall use or disclose PHI related to reproductive health care based on the presumption of lawfulness unless one of these conditions is met.

5.2 **Attestation.** If Business Associate receives a request for PHI for any of the following purposes: health oversight activities, judicial and administrative proceedings, law enforcement purposes, or disclosures to coroners and medical examiners; and the request may involve PHI related to reproductive health care, Business Associate will, without undue delay, forward such request to the Covered Entity so that the Covered Entity can review the request and the Covered Entity can respond to the request by obtaining the legally required signed attestation from the requesting party confirming that the use or disclosure is not for a prohibited reproductive health care purpose.

6. **Access to PHI.** Without undue delay following a written request from Covered Entity to Business Associate for access to PHI about an individual contained in a Designated Record Set (as such Set is defined by HIPAA regulation), the Business Associate will make available to Covered Entity, or to the individual to whom such PHI relates or his or her authorized representative, such PHI for so long as such information is maintained in the Designated Record Set as outlined in 45 C.F.R. § 164.524, or Business Associate will outline to Covered Entity how it or the individual can access such PHI on its own. If any individual requests access to PHI directly from the Business Associate, the Business Associate will, without undue delay, forward such request to the Covered Entity. Covered Entity shall be responsible for determining whether to deny access to the PHI and Business Associate will endeavor to comply with such determinations.

7. **Amendment of PHI.** Without undue delay following a written request from Covered Entity to Business Associate for the amendment of an individual's PHI or a record regarding an individual contained in a Designated Record Set the Business Associate will endeavor, as required by 45 C.F.R. § 164.526, incorporate any such amendments in the PHI. The obligation in this Section shall apply only for so long as the Business Associate maintains the PHI in a Designated Record Set. If any individual requests access to PHI directly from the Business Associate, the Business Associate will, without undue delay, forward such request to the Covered Entity.

8. **Accounting for Disclosures of PHI.** Business Associate will maintain a record of any disclosure of PHI to a third party for a purpose other than Treatment, Health Care Operations, Payment, or under an authorization

signed by the individual or personal representative of the individual who is the subject of the record. To the extent that Business Associate provides an electronic health record to Covered Entity's enrollees or customers, Business Associate shall comply with the requirements of 42 U.S.C. § 17935(c) and the regulations promulgated thereunder. Without undue delay (ideally within thirty (30) days) of written notice by Covered Entity to the Business Associate that it has received a request for an accounting of disclosures of PHI regarding an individual, the Business Associate will make available to Covered Entity such information as is in the Business Associate's possession and is required for Covered Entity to make the accounting required by 45 C.F.R. § 164.528. Business Associate will provide such information in electronic form, where available in such form. If the request for an accounting is delivered directly to the Business Associate, the Business Associate will, without undue delay, forward such request to the Covered Entity. Covered Entity shall be responsible for preparing and delivering any such accounting to the individual.

9. **Access to Books and Records Regarding PHI.** Upon the written request received by the Business Associate and if required by law, the Business Associate will make its internal practices, books, and records relating to the use and disclosure of NPI received from or created or received by the Business Associate on behalf of, Covered Entity available to the Secretary for purposes of determining compliance with HIPAA, ARRA, GLBA or any other similar statute and available to Covered Entity to ensure compliance with this BAA.

9. **Defense of Third-Party Claims.** Each party hereby agrees to defend the other party, and such other party's affiliates, officers, directors, members, employees, and agents, from and against all third-party claims arising from a breach of this BAA by the breaching party and shall pay the amounts awarded to such third party by a court competent jurisdiction. In no event shall either party be liable for indirect or consequential damages.

10. **Amendment.** The parties agree to amend this BAA, in form and substance reasonably acceptable to each party, to the extent necessary to allow either party to comply with the Privacy Rule, the Standards for Electronic Transactions (45 C.F.R. Parts 160 and 162), and the Security Standards (45 C.F.R. Part 142) including any changes required by the ARRA. Additionally, Covered Entity may update this BAA from time to time in accordance with Section 9.5 of the HealthJoy Terms and Conditions. The most current version of this Agreement will be posted on https://healthjoy.com/legal (the "Site").

11. **Term and Termination.** This BAA shall remain in effect for as long as the Business Associate provides the Program and related services to the Covered Entity. If the Covered Entity believes that Business Associate has breached any provision contained in the BAA, the Covered Entity shall provide written notice to the Business Associate detailing such breach, and if the Business Associate is not able to cure such breach or show there was no breach within 30 calendar days, then the Covered Entity may provide separate written notice to the Business Associate of its desire to terminate this BAA and the underlying Terms and Conditions at the end of the 30 day period following such second notice.

12. **Effects of Termination.** Upon the written request from Covered Entity to Business Associate and subject to required retention periods as required by applicable law, the Business Associate, and its subcontractors, will destroy or de-identify all NPI received from the Covered Entity, which the Business Associate and its subcontractors or agents still maintain in any form. Business Associate shall extend the protections, limitations, and restrictions of this BAA to the NPI retained after the termination and shall limit further disclosures to those purposes that make the return or destruction of the NPI infeasible. This provision shall survive termination of this BAA.

13. **Survival.** All Sections of this BAA that relate to Business Associate's obligations related to the privacy and security of NPI shall survive termination of this BAA for as long as Business Associate maintains NPI received or created in connection with this BAA.

14. **Third Party Beneficiaries**. Nothing in this BAA shall confer upon any person other than the parties and their respective successors or assigns, any right, remedies, obligations, or liabilities.

15. **Governing Law.** This BAA shall be governed in all respects, whether as to validity, construction, capacity, performance or otherwise, by the laws of Illinois and applicable federal law.

*****