Business Associate Agreement

This Business Associate Agreement (the "**BAA**"), effective as of the date of the last signature, is entered into by and between CLIENT ("**Covered Entity**") and Wellness IQ (the "**Business Associate**") (each a "**Party**" and collectively the "**Parties**").

Recitals

WHEREAS, the purpose of this BAA is to assure the privacy and security of Protected Health Information and Electronic Protected Health Information in accordance with the regulations (the "HIPAA Rules") issued by the Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act of 1996 as codified at 42 U.S.C. §1320d ("HIPAA") as amended by the Health Information Technology for Economic and Clinical Health Act as codified at 42 U.S.C.A. prec. § 17901 ("HITECH"), enacted as part of the American Recovery and Reinvestment Act ("ARRA"); and

WHEREAS, Covered Entity has engaged Business Associate to perform services on its behalf;

WHEREAS, Covered Entity possesses Individually Identifiable Health Information that is protected under HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations and the HITECH Standards and is permitted to use or disclose such information only in accordance with such laws and regulations;

WHEREAS, Business Associate may receive such information from Covered Entity or create and receive such information on behalf of Covered Entity;

WHEREAS, Covered Entity wishes to ensure that Business Associate will appropriately safeguard Individually Identifiable Health Information;

NOW THEREFORE, for good and valuable consideration, the sufficiency of which we hereby acknowledge, the Parties agree as follows:

1. Definitions

1.1 **Catch-all definitions**. The following terms used in this BAA shall have the same meaning as those terms in HIPAA, the HITECH Act, and any current and future regulations promulgated under HIPAA or HITECH: Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

1.2 **Specific definitions**:

(a) **Breach**. "Breach" shall mean the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted under 45 C.F.R. Part 164, Subpart E (the "HIPAA Privacy Regulations") which compromises the security or privacy of the Protected Health Information. "Breach" shall not include:

(i) Any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of Covered Entity or Business Associate, if such acquisition, access or use was made in

good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Regulations; or

(ii) Any inadvertent disclosure by a person who is authorized to access Protected Health Information at Covered Entity or Business Associate to another person authorized to access Protected Health Information at Covered Entity or Business Associate, respectively, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Regulations; or

(iii) A disclosure of Protected Health Information where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(b) **Business Associate**. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the Party to this BAA, shall mean the person/entity named above.

(c) **Covered Entity**. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the Party to this BAA, shall mean the entity named above.

(d) **Electronic Protected Health Information**. "Electronic Protected Health Information" shall mean Protected Health Information that is transmitted by or maintained in electronic media as defined by the HIPAA Security Regulations.

(e) **HIPAA Rules**. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

(f) **HITECH Standards**. "HITECH Standards" shall mean the privacy, security and security Breach notification provisions applicable to a Business Associate under Subtitle D of the HITECH Act and any regulations promulgated thereafter.

(g) **Individually Identifiable Information**. "Individually Identifiable Information" means information that is a subset of health information, including demographic information collected from an individual, and:

(i) is created or received by a health care provider, health plan, employer or health care clearinghouse; and

(ii) relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and

a. that identifies the individual; or

b. with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

2. Obligations and Activities of Business Associate

2.1 **Limited Use or Disclosure of PHI.** To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164,

Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s). Business Associate further agrees not use or disclose Protected Health Information other than as permitted or required by the BAA, in furtherance of the services provided by Business Associate for Covered Entity, or as required by law. Business Associate will not sell Protected Health Information and Electronic Health Records or use or disclose Protected Health Information for marketing or fundraising purposes as set forth in 42 U.S.C. § 17935(d) or 42 U.S.C. § 17936(a), respectively. The Business Associate shall secure Protected Health Information in accordance with 42 U.S.C. § 17932(h) and the related regulations at 45 CFR Part 164, subpart D, as well as any guidance issued by the Secretary that specifies secure technologies and methodologies such that Unsecured Protected Health Information is not maintained by the Business Associate.

2.2 **Safeguards**. The Business Associate shall implement and use appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by this BAA, including establishing procedures that limit access to PHI within its organization to those employees with a need to know the information. The Business Associate agrees that it will implement reasonable administrative, physical, and technical safeguards to protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains or transmits on behalf of the Covered Entity, as required by the HIPAA Rules.

Business Associate acknowledges and agrees that the administrative, physical and technical safeguards requirements of 45 CFR Sections 164.308, 164.310 and 164.312 shall apply to the Business Associate in the same manner that such sections apply to the Covered Entity. The Business Associate shall comply with the provisions of 45 CFR Part 164, Subpart C of the HIPAA Rules with respect to Electronic PHI to prevent any use or disclosure of PHI other than as permitted by this BAA, and shall implement and maintain in written form reasonable and appropriate policies and procedures to comply with the standards, implementation specifications or other requirements of the HIPAA Rules, in accordance with 45 CFR. Section 164.316.

2.3 **Notice of Use, Disclosure, Security Incident or Breach**

(a) Business Associate agrees to notify the designated Privacy Officer of the Covered Entity of any use or disclosure of Protected Health Information by Business Associate not provided for by the BAA, including breaches of Unsecured Protected Health Information as required at 45 CFR 164.410, and any security incident of which it becomes aware without unreasonable delay, but in no case more than thirty (30) days following discovery of breach, including instances in which an agent or subcontractor has improperly used or disclosed PHI. For purposes of this BAA, a Breach shall be treated as discovered as of the first day that the Business Associate knows of, or should reasonably have known of such Breach. Business Associate further agrees to provide the following information in such notice to Covered Entity:

(i) the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach;

(ii) a description of the nature of the Breach including the types of Unsecured Protected Health Information that were involved, the date of the Breach and the date of discovery;

(iii) a description of the type of Unsecured Protected Health Information acquired, accessed, used or disclosed in the Breach (e.g., full name, social security number, date of birth, etc.);

(iv) the identity of the person who made and who received (if known) the unauthorized acquisition, access, use or disclosure;

(v) a description of what the Business Associate is doing to mitigate the damages and protect against future breaches; and

(vi) any other details necessary for Covered Entity to assess risk of harm to Individual(s), including identification of each Individual whose Unsecured Protected Health Information has been Breached and steps such Individuals should take to protect themselves.

(b) Covered Entity will be responsible for providing notification to Individuals whose Unsecured Protected Health Information has been disclosed, as well as the Secretary and the media, as required by the HITECH Standards.

(c) Business Associate agrees to establish procedures 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.

(d) The Parties agree that this section satisfies any notice requirements of Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. For purposes of this BAA, "Unsuccessful Security Incidents" include activity such as 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 no such incident results in unauthorized access, use or disclosure of Electronic Protected Health Information.

2.4 **Mitigation**. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Association in violation of this BAA.

2.5 **Subcontractors**. Business Associate agrees to act in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, to ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

2.6 **Access**. Within ten (10) business days of a request by the Covered Entity for access to PHI about an Individual maintained by Business Associate in a Designated Record Set, the Business Associate shall make available to the Covered Entity such PHI for so long as such information is maintained in a Designated Record Set. In the event any Individual requests access to PHI directly from such Business Associate, the Business Associate shall notify Covered Entity and respond to the request for PHI within fifteen

(15) business days. If the requested PHI is maintained electronically, Business Associate must provide a copy of the PHI in the electronic form and format requested by the Individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual. Any denials of access to the PHI requested shall be the responsibility of Covered Entity. Business Associate may charge Covered Entity or Individual for the actual labor cost involved in providing such access.

2.7 **Security of Electronic Protected Health Information**. Business Associate agrees to implement administrative, physical and technical safeguards that are reasonably and appropriately designed to protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Covered Entity; (2) ensure that any agent, including a subcontractor, to whom it provides such information agrees in writing to implement reasonable and appropriate safeguards to protect it; and (3) report to the Covered Entity any security incidents of which it becomes aware in accordance with Section 2.3.

2.8 **Minimum Necessary**. Business Associate agrees to limit its uses and disclosures of, and requests for, Protected Health Information (a) when practical, to the information making up a Limited Data Set; and (b) in all other cases subject to the requirements of 45 CFR 164.502(b) and 42 U.S.C. § 17935(b), to the minimum amount of Protected Health Information necessary to accomplish the intended purpose of the use, disclosure or request.

2.9 **Amendments**. 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, upon request of Covered Entity or an Individual, pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526 within thirty (30) days.

2.10 **Accounting**. The Business Associate agrees to maintain and make available to the Covered Entity an accounting of disclosures of PHI made by Business Associate as would be required for the Covered Entity to respond to a request by an Individual made in accordance with 45 CFR 164.528. At a minimum, the accounting of disclosures shall include the following information:

(a) Date of disclosure;

(b) The name of the person or entity who received the PHI, and if known, the address of such entity or person;

(c) A brief description of the PHI disclosed; and

(d) A brief statement of the purpose of such disclosure which includes an explanation of the basis of such disclosure.

In the event the request for an accounting is delivered directly to the Business Associate, the Business Associate shall notify the Covered Entity and respond to the request within fifteen (15) business days. Any denials of a request for an accounting shall be the responsibility of Covered Entity. The Business Associate agrees to implement an appropriate recordkeeping process to enable it to comply with the requirements of this Section.

Business Associate need not record disclosure information or otherwise account for disclosures of PHI that this BAA or Covered Entity in writing permits or requires (i) for the purpose of Covered Entity's treatment activities, payment activities, or health care operations (except where such recording or accounting is required by the HITECH Act, and as of the effective dates for this provision of the HITECH Act); (ii) to the individual who is the subject of the PHI disclosed or to that individual's personal representative; (iii) to persons involved in that individual's health care or payment for health care; (iv) for notification for disaster relief purposes; (v) for national security or intelligence purposes; (vi) to law enforcement officials or correctional institutions regarding inmates; or (vii) pursuant to an authorization.

2.11 **Disclosure of Practices, Books and Records**. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, available to Covered Entity or the Secretary in a time or manner designated by the Covered Entity or Secretary, for purposes of determining compliance with the HIPAA Rules.

3 Permitted Uses and Disclosures by Business Associate

3.1 **Permitted Use and Disclosure**. Except as otherwise limited in this BAA, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity provided that such use or disclosure would not violate the HIPAA Rules.

(a) Business Associate may use or disclose Protected Health Information as necessary to perform and in furtherance of the services to Covered Entity, which may include use and disclosure in databases, software and aggregation services available to Business Associate.

(b) Business Associate is authorized to use Protected Health Information to de-identify the information in accordance with 45 CFR 164.514(a)-(c).

(c) Business Associate may use or disclose Protected Health Information as required by law. Business Associate shall disclose the minimum amount necessary to satisfy the requirement and shall make reasonable efforts to obtain assurances that confidential treatment be accorded to Protected Health Information.

(d) Business Associate agrees to limit its uses and disclosures of, and requests for, Protected Health Information (i) when practical, to the information making up a Limited Data Set; and (ii) in all other cases to the minimum amount of Protected Health Information necessary to accomplish the intended purpose of the use, disclosure or request.

3.2 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

4 Obligations of Covered Entity

4.1 **Notice of Privacy Practices of Covered Entity**. Covered Entity shall notify Business Associate in writing of any limitation(s) in the notice of privacy practices of covered

entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

4.2 **Restrictions in Use of Protected Health Information**. Covered Entity shall notify Business Associate in writing 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.

4.3 **Changes in the Use of Protected Health Information**. 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 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

4.4 **Permissible Requests by Covered Entity**. Except as otherwise provided in this BAA, Covered Entity will not ask Business Associate to use or disclose Protected Health Information in any manner that would violate the HIPAA Rules or the HITECH Standard if done by Covered Entity

5 Term and Termination

5.1 **Term**. The initial term of this BAA shall begin on the Effective Date and continue for one year from the Effective Date. Thereafter this BAA shall continue until either party provides the other ninety (90) days written notice to terminate or on the date either party terminates for cause as authorized in Section 5.2, whichever is sooner.

5.2 **Termination for Cause**. Upon either Party's reasonable determination that the other Party has committed a violation or material breach of this BAA, the non-breaching Party may take one of the following steps:

(a) Provide an opportunity for the breaching Party to cure the breach or end the violation, and if the breaching Party does not cure the breach or end the violation within thirty (30) days, terminate this BAA;

(b) Immediately terminate this BAA if the other Party has committed a material breach of this BAA and cure of the material breach is not possible as acknowledged by both parties; or

(c) If neither cure nor termination is feasible, elect to continue this BAA and report the violation or material breach to the Secretary in accordance with the requirements set forth in the HIPAA Rules.

5.3 **Obligations of Business Associate Upon Termination**. Upon termination of this BAA for any reason, Business Associate, with respect to Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

(a) 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;

(b) Return to Covered Entity or destroy the remaining Protected Health Information that the Business Associate still maintains in any form;

(c) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR 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 the Protected Health Information;

(d) Not use or disclose the 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 3.1 which applied prior to termination; and

(e) Return to Covered Entity or, if agreed to by Covered Entity, destroy the 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.

(f) Notwithstanding anything to the contrary herein, Covered Entity authorizes Business Associate to transmit Protected Health Information to another business associate of Covered Entity.

5.4 **Survival**. The obligations of Business Associate under this Section shall survive the termination of this BAA.

6 Miscellaneous

6.1 **Regulatory References**. A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.

6.2 **Amendment**. The Parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

6.3 **Interpretation**. Any ambiguity in this BAA shall be interpreted to permit compliance with the HIPAA Rules.

6.4 **Prior Agreement**. This BAA shall replace and supersede any prior Business Associate Agreement between the Parties.

6.5 **Indemnification**. Each Party shall indemnify and hold harmless the other Party and its affiliates, directors, officers, employees, partners, contractors or agents, from and against any and all claims, actions, causes of action, demands, or liabilities of whatsoever kind and nature, including judgments, interest, reasonable attorneys' fees, and all other costs, fees, expenses, and charges (collectively, "Claims") to the extent that such Claims arise out of or were caused by the negligence or willful misconduct of the indemnifying Party or from any material breach of the BAA by the indemnifying Party, unless such Claims arose from or were caused by the negligence or willful misconduct of the party seeking indemnification hereunder.