This Business Associate Partner Agreement ("Agreement") is made a part of the AlayaCare Partnership Agreement ("Underlying Agreement").

Business Associate and Partner wish to enter into this Agreement to comply with the requirements of (i) the implementing regulations at 45 C.F.R Parts 160, 162, and 164 for the United States Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*i.e.,* the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("the Implementing Regulations"), (ii) the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act"), and (iii) the requirements of the final modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules as issued on January 25, 2013 and effective March 26, 2013 (75 Fed. Reg. 5566 (Jan. 25, 2013)) ("the Final Regulations"). The Implementing Regulations, the HITECH Act, and the Final Regulations are collectively referred to in this Agreement as "the HIPAA Requirements."

Business Associate and Partner agree to incorporate into this Agreement any regulations issued by the U.S. Department of Health and Human Services ("HHS") with respect to the HIPAA Requirements that relate to the obligations of Partners to be reflected in a Business Associate Partner Agreement. Partner recognizes and agrees that it is obligated by law to meet the provisions of the HIPAA Requirements directly applicable to Partner, and that it has direct liability for any violations of such HIPAA Requirements.

In the event of an inconsistency between the provisions of this Agreement and a mandatory term of the HIPAA Requirements (as these terms may be expressly amended from time to time by HHS or as a result of interpretations by HHS, a court, or another regulatory agency with authority over the parties), the interpretation of HHS, such court or regulatory agency shall prevail.

Where provisions of this Agreement are different from those mandated by the HIPAA Requirements, but are nonetheless permitted by the HIPAA Requirements, the provisions of this Agreement shall control.

In the event of an inconsistency between the Agreement and any other agreement currently in effect between the parties, the provisions of this Agreement shall control with respect to the subject matter contained herein.

In light of the foregoing and the requirements of HIPAA, Partner and Business Associate agree to be bound by the following terms and conditions:

1. **Definitions.**

(a) General. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms are defined in the HIPAA Requirements.

(b) Specific.

i. Breach. "Breach" shall mean, as defined in 45 C.F.R. § 164.402, the acquisition, access, use or disclosure of Unsecured Protected Health Information in a manner not permitted by the HIPAA Requirements that compromises the security or privacy of that Protected Health Information.

ii. Partner. "Partner" shall generally have the same meaning as the term "business associate" at 45 C.F.R. §160.103 in the context of creating, receiving, maintaining, or transmitting Protected Health Information on behalf of a Covered Entity.

iii. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. §160.103, and in reference to the party to this Business Associate Partner Agreement, shall include any client of Business Associate or Partner who uses the services of Business Associate or Partner to create, receive, maintain or transmit EPHI.

iv. Electronic Protected Health Information. "Electronic Protected Health Information" ("EPHI") shall have the same meaning set forth in 45 C.F.R. § 160.103, as amended from time to time, and generally means Protected Health Information that is transmitted or maintained in any electronic media.

v. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

vi. Privacy Rule. "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.

vii. Protected Health Information. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 CFR §160.103, limited to the information created, received, maintained, or transmitted by Partner from or on behalf of Business Associate pursuant to this Agreement.

viii. Required By Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501.

ix. Security Incidents. The term "Security Incidents" has the meaning set forth in 45 C.F.R. § 164.304, as amended from

time to time, and generally means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

x. Security Rule. "Security Rule" shall mean the Standards for Security of Individually Identifiable Health Information created, transmitted, maintained or received in an electronic media (45 C.F.R. Parts 160, 162 and 164.)

xi. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

xii. Unsecured Protected Health Information. "Unsecured Protected Health Information" shall mean, as defined in 45 C.F.R. §164.402, Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HHS.

2. **Flow-Down of Obligations to Downstream Entities**. Partner agrees that as required by the HIPAA Requirements, Partner will enter into a written agreement with all entities with which Partner has contracted that will create, receive, maintain or transmit PHI ("Downstream Entities"). The agreement shall: (i) require the Downstream Entities to comply with the Privacy and Security Rule provisions of this Agreement in the same manner as required of Partner, and (ii) notify such Downstream Entities that they will incur liability under the HIPAA Requirements for non-compliance with such provisions. Accordingly, Partner shall ensure that all Downstream Entities agree in writing to the same privacy and security restrictions, conditions and requirements that apply to Partner with respect to PHI.

3. **Obligations and Activities of Partner under HIPAA Privacy Rules.**

(a) Use and Disclosure. Partner agrees to not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law. When performing functions and activities for Business Associate, Partner agrees to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request.

(b) Appropriate Safeguards. Partner shall establish, implement and maintain appropriate safeguards, and comply with the Security Standards (Subpart C of 45 C.F.R. Part 164) with respect to electronic PHI, as necessary to prevent any use or disclosure of PHI other than as provided for by this Agreement. Without limiting the generality of the foregoing, Partner agrees to protect the integrity and confidentiality of any PHI it electronically exchanges with Business Associate.

(c) Mitigation. Partner agrees to mitigate, to the extent practicable, any harmful effect that is known to Partner of a use or disclosure of PHI by Partner in violation of the requirements of this Agreement.

(d) Reporting. Partner shall report to Business Associate any use or disclosure of PHI that is not provided in this Agreement of which Partner becomes aware, including reporting Breaches of Unsecured PHI as required by 45 C.F.R. § 164.410 and this Agreement.

(e) Access to Designated Record Sets. To the extent that Partner possesses or maintains PHI in a Designated Record Set, Partner agrees to provide access, at the request of Business Associate, and in the time and manner reasonably requested by Business Associate, to PHI in a Designated Record Set, to Business Associate or, as directed by Business Associate, to those individuals who are the subject of the PHI (or their designees). Partner shall make such information available in an electronic format where directed by Business Associate.

(f) Amendments to Designated Record Sets. To the extent that Partner possesses or maintains PHI in a Designated Record Set, Partner agrees to make any amendment(s) to PHI in a Designated Record Set that the Business Associate directs or agrees to, at the request of Business Associate or an Individual, and in the time and manner reasonably requested by Business Associate.

(g) Access to Books and Records. Partner agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Partner on behalf of, Business Associate available to Business Associate, or to the Secretary, in a time and manner reasonably requested by the Business Associate or designated by the Secretary, for purposes of the Secretary determining Business Associate's and/or Partner's compliance with the HIPAA Requirements.

(h) Accountings. Partner agrees to document such disclosures of PHI and information related to such disclosures as would be required for Business Associate to respond to a request by an Individual for an accounting of disclosures of PHI.

(i) Requests for Accountings. Partner agrees to provide to Business Associate, in the time and manner reasonably requested by Business Associate, information collected in accordance with Section 3.h. of this Agreement, to permit Business Associate to respond to a request by an Individual for an accounting of disclosures of PHI.

4. Obligations and Activities of Partner under HIPAA Security Rules.

(a) Partner shall use appropriate administrative, technical, and physical safeguards ("Safeguards"), that reasonably and appropriately protect the integrity, confidentiality, and availability of, and to prevent non-permitted or violating use or disclosure of, EPHI created, transmitted, maintained, or received in connection with the services provided to Business Associate.

(b) Partner shall document and keep these Safeguards current. These Safeguards shall extend to transmission, processing, and storage of EPHI. Transmission of EPHI shall include transportation of storage media, such as magnetic tape, disks or

compact disk media, from one location to another. Upon Business Associate's request, Partner shall provide Business Associate access to, and copies of, documentation regarding such Safeguards.

(c) Partner shall comply with and implement the requirements of the HIPAA Security Rule (45 C.F.R. Parts 160, 162, and 164) by:

i. Implementing administrative, physical, and technical safeguards required by the Security Rule that reasonably protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf of Business Associate.

ii. Ensuring that any Downstream Entities to whom it provides such information agree to implement reasonable and appropriate safeguards to protect such information;

iii. Reporting and tracking all Security Incidents as described below:

iv. Partner shall report to Business Associate any Security Incident that results in (i) unauthorized access, use, disclosure, modification, or destruction of Business Associate's EPHI of which Partner becomes aware, or (ii) interference with Partner's system operations in Partner's information systems, of which Partner becomes aware;

v. Partner shall report to Business Associate within five days after Partner learns of such Security Incident. For any other Security Incident, Partner shall aggregate the data and provide such reports on a quarterly basis, or more frequently upon Business Associate's request.

vi. Making Partner's policies and procedures and documentation required by the Security Rule related to these safeguards available to the Secretary for purposes of determining Business Associate's and/or Partner's compliance with the Security Rule.

(d) Partner agrees to take all reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to Partner resulting from any unauthorized access, use, disclosure modification or destruction of EPHI.

5. Notice and Reporting Obligations of Partner.

(a) Partner shall notify Business Associate within five days after discovery by Partner, any unauthorized access, use, disclosure, modification, or destruction of PHI (including any successful Security Incident) that is not permitted by this Agreement, by applicable law, or permitted in writing by Business Associate, whether such non-compliance is by Partner or a Downstream Entity.

(b) Partner shall, as required by law, notify Business Associate of the discovery of any Breach of Unsecured Protected Health Information by Partner or a Downstream Entity. Notice must be made without any unreasonable delay and no later than five days after discovery of the Breach by Partner.

(c) As provided for in 45 C.F.R. Sec. 164.402, Partner recognizes and agrees that any acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under the HIPAA Privacy Rule (Subpart E of 45 C.F.R. Part 164) is presumed to be a Breach. As such, Partner shall assist Business Associate in performing a risk assessment to examine whether there is a low probability that the Unsecured PHI has been compromised.

In connection with its notification of a Breach to Business Associate, Partner shall:

- Identify each individual (if known) whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired, or disclosed.
- Identify the nature of the Breach, including the date of the Breach and date of the discovery.
- Identify the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- Identify the unauthorized person who used the PHI or to whom the disclosure was made.
- Determine whether the PHI was actually acquired or viewed.
- Identify what corrective or investigational action Partner took or will take to prevent further non-permitted accesses, uses, or disclosures.
- Determine the extent to which the risk to the PHI has been or will be mitigated by Partner.
- Determine whether the incident falls under any of the Breach notification exceptions.

6. **Permitted Uses and Disclosures by Partner.**

(a) Agreement. Partner agrees to create, receive, use, disclose, maintain or transmit PHI only in a manner that is consistent with this Agreement or the HIPAA Requirements, and only in connection with the services to be provided to Business Associate. To that end, Partner may not use or disclose PHI in a manner that would violate the requirements of the Privacy Rule if done by Business Associate, subject to subsections 6(b) and (c), or the minimum necessary policies and procedures of Business Associate.

(b) Use for Administration of Partner. As permitted by the HIPAA requirements, Partner may use PHI received by the Partner in its capacity as a Partner to the Business Associate for 1) the proper management and administration of the Partner or to carry out the legal responsibilities of the Partner, or 2) data aggregation services relating to health care operations of

the Business Associate.
(c) Disclosure for Administration of Partner. As permitted by the HIPAA Requirements, Partner may disclose PHI received by the Partner in its capacity as a Partner to the Business Associate for the proper management and administration of the Partner, provided that disclosures are Required by Law, or Partner obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies the Partner of any instances of which it is aware in which the confidentiality of the information has been breached.

7. **Permissible Requests by Business Associate.**
Except as set forth in Section 6 of this Agreement, Business Associate shall not request Partner to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Business Associate.

8. **Term and Termination.**
(a) Term. This Agreement shall be effective as of September 23, 2013 and shall terminate when all of the PHI provided by Business Associate to Partner, or created or received by Partner on behalf of Business Associate, is destroyed or returned to Business Associate, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
(b) Termination for Cause. Upon either party's knowledge of a material breach by the other party, including the breaching party engaging in a pattern of activity or practice that constitutes a material breach or violation of the breaching party's obligations under this Agreement, the non-breaching party shall either:
i. Provide an opportunity for the breaching party to cure the breach or end the violation. If the breaching party does not cure the breach or end the violation within the time specified by the non-breaching party, the non-breaching party shall terminate this Agreement;
ii. Immediately terminate this Agreement if the breaching party has breached a material term of this Agreement and cure is not possible; or
iii. If neither termination nor cure are feasible, the breaching party shall report the violation to the Secretary.
(c) Effect of Termination.
i. Except as provided in paragraph ii. of this Section 8.c., upon termination of the services provided to Business Associate under the Agreement, for any reason, Partner shall return or destroy all PHI received from Business Associate , or created, maintained, or received by Partner on behalf of Business Associate. This provision shall apply to PHI that is in the possession of Downstream Entities. Partner shall retain no copies of the PHI.
ii. In the event that Partner determines that returning or destroying the PHI is infeasible, Partner shall provide to Business Associate notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Partner shall extend the protections of this Agreement and the HIPAA Requirements to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Partner maintains such PHI.

9. **Miscellaneous.**
(a) Regulatory References. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.
(b) Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Business Associate to comply with the requirements of the Privacy Rule, the Security Rule and HIPAA.
(c) Survival. Partner's and Business Associate's obligation to protect the privacy and security of the PHI they created, received, maintained, or transmitted in connection with the services provided will be continuous and survive termination, cancellation, expiration, or other conclusion of this Agreement.
(d) Information Systems. If Partner is provided access to any Business Associate information system or network containing any EPHI, Partner agrees to comply with all Business Associate policies for access to and use of information from the information systems or network
(e) Interpretation. Any ambiguity in this Agreement shall be resolved to permit Business Associate to comply with the applicable provisions of the Privacy Rule and Security Rule.
(f) No Third Party Beneficiaries. Nothing in this Agreement shall be construed as creating any rights or benefits to any third parties.
Miscellaneous. The Agreement constitutes the entire agreement between the parties with respect to the subject matter contained herein, and no other representations, oral or otherwise, are binding.