CONFIDENTIALITY and HIPAA PRIVACY BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT is entered into by and among **[Insert Client Name here]** ("**Client**"), who maintains a self-insured medical plan that is a signatory to this Agreement, the **[Insert Name of Plan]** ("**Plan**"), and **[Insert Humana Entity Name]** ("**Business Associate**"), who is a provider of administrative services with respect to the Plan under a separate agreement referred to as the "ASO Agreement".
.

WITNESSETH

WHEREAS, Plan and Business Associate desire to enter into a HIPAA Business Associate Agreement (hereinafter the "Agreement) as follows:

Scope of Agreement

A. In conformity with the regulations at 45 C.F.R. Parts 160-164 (the "Privacy and Security Rules"), Plan will provide Business Associate with access to, or have Business Associate create, maintain, transmit and/or receive certain Protected Health Information ("PHI" as defined below), thus necessitating a written agreement that meets the applicable requirements of the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and the American Recovery and Reinvestment Act of 2009 ("ARRA" as defined below).

B. Plan and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to this Agreement in compliance with HIPAA and the regulations promulgated thereunder by the U.S. Department of Health and Human Services, including, but not limited to, Title 45, Section 164.504(e) of the Code of Federal Regulations ("CFR" as defined below), as the same may be amended from time to time and other applicable state and federal laws, rules and regulations regarding privacy and security of personal information.

C. The parties acknowledge that state and federal laws relating to electronic data security and privacy are rapidly evolving and that further amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, ARRA, and other applicable state and federal laws relating to the security or confidentiality of PHI.

D. In the event of any conflict between this Agreement and the Arrangement as to the subject matter referenced herein, this Agreement shall control.

In consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

1. Definitions. The following terms shall have the meaning set forth below:

(a) ARRA. "ARRA" means the American Recovery and Reinvestment Act of 2009

(b) Business Associate. "Business Associate" means a person or entity, other than a member of the workforce of a Plan, who performs functions or activities on behalf of, or provides certain services to, a Plan that involve access by the business associate to protected health information.

(c) C. F. R. "C.F. R." means the Code of Federal Regulations.

(d) Designated Record Set. "Designated Record Set" has the meaning assigned to such term in 45 C. F. R. 164.501.

(e) Discovery. "Discovery" shall mean the first day on which a Security Breach is known to Business Associate (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of Business Associate), or should reasonably have been known to Business Associate, to have occurred.

(f) Electronic Health Record. "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.

(g) Electronic Protected Health Information. "Electronic Protected Health Information" means information that comes within paragraphs 1 (i) or 1 (ii) of the definition of "Protected Health Information", as defined in 45 C. F. R. 160.103.

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

(i) Protected Health Information. "Protected Health Information" shall have the same meaning as the term "Protected Health Information", as defined by 45 C. F. R. 160.103, limited to the information created or received by Business Associate from or on behalf of Plan.

(j) Required by Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 C. F. R. 164.501.

(k) Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

(l) Security Breach. "Security Breach" means the unauthorized acquisition, access, use or disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Security Breach does not include:

(i) any unintentional acquisition, access, or use of Protected Health Information by an employee or individual acting under the authority of Business Associate if:

(a) such acquisition, access or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with Business Associate; and

(b) such information is not further acquired, accessed, used or disclosed by any person; or

(ii) any inadvertent disclosure from an individual who is otherwise authorized to access Protected Health Information at a facility operated by Business Associate to another similarly situated individual at the same facility; and

(iii) any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person.

(m) Security Incident. "Security Incident" shall have the same meaning as the term "security incident" in 45 C. F. R. 164.304.

(n) Standard Transactions. "Standard Transactions" means the electronic health care transactions for which HIPAA standards have been established, as set forth in 45 C. F. R., Parts 160-162.

(o) Subcontractor. "Subcontractor" means a person to whom business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

(p) Terms. All other terms used, but not defined, shall have the same meaning as those terms are given in 45 C.F.R. 160-164.

(q) Unsecured Protected Health Information. "Unsecured Protected Health Information" shall have the meaning as the term "unsecured protected health information" in 45 C.F.R. 164.402.

2. Obligation of Business Associate.

(a) **Permitted Uses and Disclosures**. Business Associate may create, use and/or disclose the Plan's PHI pursuant to the ASO Agreement or this Agreement only in accordance with the specifications set forth in the underlying ASO Agreement, this Agreement or as Required by Law provided that such use or disclosure would not violate the Privacy and Security Rules if done by Plan

(b) **Specific Use and Disclosure Provisions**

(1) Except as otherwise prohibited by this Agreement, 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.

(2) Except as otherwise prohibited by this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances, in the form of a business associate agreement, from the person or entity 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 or entity, and the person or entity notifies the Business Associate of any instances of which it is aware the confidentiality of the information has been breached in accordance with the Security Breach and Security Incident notifications requirements of this Agreement.

(3) Business Associate will afford access to Protected Health Information or other personal information received by it to the Plan or the Client, as permitted under this Agreement and by law. Business Associate will afford access to this information to other persons only as reasonably directed in writing by Plan or the Client, with due regard for confidentiality, and Business Associate shall have no further obligation with respect to that information. Except as provided in this Agreement, Business Associate will disclose Protected Health Information to a third party only if authorized by an ancillary agreement respecting confidentiality. Business Associate is directed to afford access to Protected Health Information to the persons listed in Attachment A, under circumstances where disclosure is appropriate and necessary:

(4) Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an Individual without the Plan's prior written approval and notice from Plan that it has obtained from the Individual, in accordance with 45 C.F.R. 164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by Business Associate. The foregoing shall not apply to Plan's payments to Business Associate for services delivered by Business Associate.

(5) Except as otherwise prohibited by this Agreement, Business Associate may use Protected Health Information to provide data aggregation services to Plan as permitted by 42 C.F.R. 164.504(e)(2)(i)(B).

(6) Business Associate may use Protected Health Information to report violation of law to appropriate Federal and State authorities, consistent with 164.502 (j)(1).

(7) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Plan except for the specific uses and disclosures set out above in this Section 2.(b).

(8) Business Associate shall not use or disclose health information in a manner that would violate 42 C.F.R. 164.522(a)(vi)(B).

(c) **Nondisclosure**. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law. Business Associate shall also comply with any further limitations on uses and disclosures agreed to by Plan in accordance with 45 C.F.R. 164.522 provided that such agreed upon limitations have been communicated to Business Associate in accordance with Section 3(d) of this Agreement.

(d) **Safeguards**. Business Associate shall use appropriate safeguards to prevent use or disclosure of PHI other than as specifically provided for by the Arrangement or this Agreement. Such safeguards shall at a minimum include: (i) a comprehensive written information privacy and security policy; and (ii) a program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of his/her/its activities; and (iii) periodic and mandatory privacy and security training and awareness to its employees and subcontractors; and (iv) appropriate confidentiality agreements with all employees, Subcontractors, independent contractors and any entity to which Business Associate has delegated or sub-delegated his/her/its rights, duties, activities and/or obligations under the Arrangement or this Agreement which contain terms and conditions that are the same or similar to those contained in this Agreement.

(e) **Reporting of Disclosures and Mitigation.** Business Associate shall provide notice to Plan of any use or disclosure of PHI other than as specifically provided for by the Arrangement or this Agreement. Such notice shall be provided in the manner set out in this Agreement. 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 Associate in violation of the requirements of this Agreement.

(f) **Contractors**. It is understood and agreed that Business Associate shall maintain written business associate agreements with Subcontractors, as necessary to perform the services required under the ASO Agreement, in a form consistent with, the terms and conditions, restrictions and requirements established in this Agreement. The business associate agreements shall require such Subcontractors to enter into additional downstream business associate agreements in order for Business Associate to comply with this Agreement and Business Associate's independent HIPAA obligations as set out in 45 C.F.R. 164.502(e)(1)(ii) and 164.308(b)(2). Business Associate agrees and shall require contractors to agree that in the event of any conflict between such business associate agreements and this Agreement, the language in this Agreement shall control. Business Associate shall ensure that any agents, including Subcontractors, to whom it provides Plan customer's PHI received from, created by, or received by Business Associate on behalf of Plan agrees to the same restrictions and conditions that apply to Business Associate with respect to such PHI.

(g) **Availability of Information.** Business Associate agrees to provide access, at the request of Plan, and in the time and manner designated by Plan, to Protected Health Information in a Designated Record Set, to Plan or, as directed by Plan, to an Individual in order to meet the requirements under 45 C.F.R. 164.524. Plan's determination of what constitutes "Protected Health Information" or a "Designated Record Set" shall be final and conclusive. If Business Associate provides copies or summaries of Protected Health Information to an Individual it may impose a reasonable, cost-based fee in accordance with 45 C.F.R. 164.524 (c)(4).

(h) **Amendment of PHI**. Business Associate shall make PHI available to Plan as reasonably required to fulfill Humana's obligations to amend such PHI pursuant to HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR Section 164.526 and Business Associate shall, as directed by Plan, incorporate any amendments to PHI into copies of such PHI maintained by Business Associate.

(i) **Internal Practices**. Business Associate agrees to make (i) internal practices, books, and records, including policies and procedures, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Plan, and (ii) policies, procedures, and documentation relating to the safeguarding of Electronic Protected Health Information available at the request of the Plan to

the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Plan's compliance with the Privacy and Security Rules.

(j) **Notification of Breach**. Beginning on the Effective Date of this Agreement, Business Associate agrees to report to Plan any potential Security Breach of Unsecured Protected Health Information without unreasonable delay and in no case later than ten (10) calendar days after Discovery of a Security Breach. Such notice shall include: (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; and (ii) a brief description of the event; and (iii) the date of the potential Security Breach; and (iv) the date of discovery; and (v) the type of Protected Health Information involved; and (vi) any preliminary steps taken to mitigate the damage; and (vii) a description of any investigatory steps taken. In addition, Business Associate shall provide any additional information reasonably requested by Planfor purposes of investigating the Security Breach. Business Associate's notification of a Security Breach under this section shall comply in all respects with each applicable provision of Section 13400 of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time.

Breach notifications must be reported to Plan by one of the following methods:

By Mail: [Plan's Privacy Officer]
[Addr 1]
[Addr 2]
[City, State, Zip]

By Phone: [Insert Phone Number]

By Email: [Insert Email address]

(k) Business Associate agrees to document such disclosures of Protected Health Information as would be required for Plan to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528.

(l) Business Associate agrees to provide to Plan, in the time and manner designated by Plan, the information collected in accordance with this Agreement, to permit Plan to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528. In addition, with respect to information contained in an Electronic Health Record, Business Associate shall document, and maintain such documentation for three (3) years from date of disclosure, such disclosures as would be required for Plan to respond to a request by an Individual for an accounting of disclosures of information contained in an Electronic Health Record, as required by Section 13405(c) of Subtitle D (Privacy) of ARRA and related regulations issued by the Secretary from time to time.

(m) Business Associate acknowledges that it shall request from Plan and so disclose to its affiliates, agents and Subcontractors or other third parties, (i) the information contained in a "limited data set," as such term is defined at 45 C.F.R. 164.514(e)(2), or, (ii) if needed by Business Associate, to the minimum necessary to accomplish the intended purpose of such requests or disclosures. In all cases, Business Associate shall request and disclose Protected Health Information only in a manner that is consistent with guidance issued by the Secretary from time to time

(n) With respect to Electronic Protected Health Information, Business Associate shall implement and comply with (and ensure that its Subcontractors implement and comply with) the administrative safeguards set forth at 45 C.F.R. 164.308, the physical safeguards set forth at 45 C.F.R. 164.310, the technical safeguards set forth at 45 C.F.R. 164.312, and the policies and procedures set forth at 45 C.F.R. 164.316 to reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Plan. Business Associate acknowledges that on the Effective Date of this Agreement, (i) the foregoing safeguard, policies and

procedures requirements shall apply to Business Associate in the same manner that such requirements apply to Plan.

(o) With respect to Electronic Protected Health Information, Business Associate shall ensure that any agent, including a Subcontractor, to whom it provides Electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it.

(p) Business Associate shall report to Plan any Security Incident of which it becomes aware. For purposes of reporting to Plan, any attempted unsuccessful Security Incident means any attempted unauthorized access that prompts Business Associate to investigate the attempt or review or change its current security measures.

(q) If Business Associate conducts any Standard Transactions on behalf of Plan, Business Associate shall comply with the applicable requirements of 45 C.F.R. Parts 160-162.

3. Obligations of Plan.

(a) Plan will use appropriate safeguards to maintain the confidentiality, privacy and security of PHI in transmitting same to Business Associate pursuant to the Arrangement and this Agreement.

(b) Plan shall notify Business Associate of any limitation(s) in Plan's notice of privacy practices that Plan produces in accordance with 45 C.F.R. 164.520 (as well as any changes to that notice), to the extent that such limitation(s) may affect Business Associate's use or disclosure of Protected Health Information.

(c) Plan shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes affect Business Associate's use or disclosure of Protected Health Information.

(d) Plan shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Plan has agreed to in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

4. Audits, Inspection and Enforcement. From time to time upon reasonable advance notice, or upon a reasonable determination by Plan that Business Associate has potentially or actually breached this Agreement, Plan, at its own expense, may inspect the facilities, systems, books, procedures and records of Business Associate to monitor compliance with this Agreement. Business Associate shall promptly remedy any violation of any term of this Agreement and shall certify the same to Plan in writing.

5. Waiver. Waiver, whether expressed or implied, of any breach of any provision of this Agreement shall not be deemed to be a waiver of any other provision or a waiver of any subsequent or continuing breach of the same provision. In addition, waiver of one of the remedies available to either party in the event of a default or breach of this Agreement by the other party, shall not at any time be deemed a waiver of a party's right to elect such remedy(ies) at any subsequent time if a condition of default continues or recurs.

6. Termination.

(a) Term. The provisions of this Agreement shall take effect on the Agreement's Effective Date and shall terminate when all of the Protected Health Information provided by Plan to Business Associate, or created, maintained, transmitted or received by Business Associate on behalf of Plan, is destroyed or returned to Plan, or, in accordance with Section 6(c)(2).

(b) Termination for Cause. Without limiting the termination rights of the parties pursuant to the Agreement and upon, either party's knowledge of a material breach of this Agreement by the other party, the nonbreaching party shall provide an opportunity for the breaching party, to cure the breach or end the violation, or terminate

the Agreement, if the breaching party does not cure the breach or end the violation within the time specified by the non-breaching party, or immediately terminate this Agreement, if, in the non-breaching party's reasonable judgment cure is not possible.

(c) Effect of Termination.

(1) Except as provided in Section 6(c), upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Plan, or created, maintained, transmitted or received by Business Associate on behalf of Plan. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event the Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Plan notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of Protected Health Information is infeasible, per Section 6(a) above, Business Associate shall continue to extend the protection of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information for so long as Business Associate maintains such Protected Health Information.

(d) Upon termination of this Agreement for any reason, Business Associate, with respect to protected health information received from Plan, or created, maintained, or received by business associate on behalf of Plan, shall:

1. 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;
2. Return to Plan the remaining Protected Health Information that the Business Associate still maintains in any form;
3. 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;
4. 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 in Section 2(b) under "Permitted Uses and Disclosures By Business Associate" which applied prior to termination; and
5. Return to Plan or 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.

(e) Judicial or Administrative Proceedings. Either party may terminate the Arrangement, effective immediately, if: (i) the other party is named as a defendant in a criminal proceeding for a violation of HIPAA or (ii) a finding or stipulation that the other party has violated any standard or requirement of HIPAA or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.

7. Indemnification. Plan and Business Associate will indemnify hold harmless and defend the other party to this Agreement from and against any and all claims, losses, liabilities, costs and other expenses incurred as a result of, or arising directly or indirectly out of or in connection with: (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of the party under this Agreement; and (ii) any claims, demands, awards, judgments, actions and proceedings made by any person or organization arising out of or in any way connected with the party's performance under this Agreement.

8. Disclaimer. Business Associate makes no warranty or representation that compliance by Plan with this Agreement, HIPAA or ARRA will be adequate or satisfactory for Plan's own purposes or that any information in Plan's

possession or control, or transmitted or received by Plan, is or will be secure from unauthorized use or disclosure. Plan is solely responsible for all decisions made by Plan regarding the safeguarding of PHI.

9. No Third Party Beneficiaries. The parties have not created and do not intend to create by this Agreement any third party rights under this Agreement, including but not limited to members. There are no third party beneficiaries to this Agreement.

10. Receipt of PHI. Business Associate's receipt of Plan member's PHI pursuant to the transactions contemplated by the Arrangement shall be deemed to begin on the execution date below, and Business Associate's obligations under this Agreement shall commence with respect to such PHI upon such receipt.

11. Interpretation. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA Regulations.

12. Regulatory References. A reference in this Agreement to a section in the Privacy and Security Rules means the section as in effect or as amended.

13. Amendment. Upon the enactment of any law or regulation affecting the use or disclosure of Protected Health Information, the safeguarding of Electronic Protected Health Information, or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, the party's shall negotiate in good faith to amend this Business Associate agreement to bring it into compliance such new law, regulation or decision of the court. If the parties are unable to agree on an amendment within thirty (30) days thereafter, then either of the parties may terminate the Agreement on thirty (30) days written notice to the other party.

14. Survival. The respective rights and obligations of Business Associate under Sections 6 and 7 of this Agreement shall survive the termination of this Agreement.

15. Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Kentucky.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement to be effective as of the Enter Day day of Enter Month, Enter Year.

Business Associate	Plan
By: _____	By:_____
Print Name:Khalid Nazir	Print Name: _____
Title: VP Finance	Title: _____
Date: _____	Date: _____

Address for Notice:	Address for Notice:
_____	_____
_____	_____
_____	_____
_____	_____

COPY TO:	COPY TO
Humana Inc.	_____
500 West Main Street	_____
Louisville, KY 40202	_____
Attn: Law Department	_____

Attachment A

Persons Authorized to Receive Protected Health Information on behalf of the Plan"

Individual's name	Individual's name
Title	Title
Company Name	Company Name
address	address
city / state / zip	city / state / zip
Telephone No.	Telephone No.
FAX No.	FAX No.
E-Mail Address	E-Mail Address

Individual's name	Individual's name
Title	Title
Company Name	Company Name
address	address
city / state / zip	city / state / zip
Telephone No.	Telephone No.
FAX No.	FAX No.
E-Mail Address	E-Mail Address

Add additional Names as Necessary