



BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement, is entered into as of _____, by and between _____ Health Plan (the "Plan" or "Covered Entity"); and BASIC Benefits, LLC ("Business Associate").

WITNESSETH:

WHEREAS, the Covered Entity previously has entered into a Master Services Agreement (the "MSA") with the Business Associate, whereby the Business Associate has agreed to provide certain services to the Plan;

WHEREAS, to provide such services to the Plan, the Business Associate must have access to certain protected health information ("Protected Health Information" or "PHI"), as defined in the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards") set forth by the U.S. Department of Health and Human Services ("HHS") pursuant to the Health Insurance Portability and Accountability Act of 1996, ("HIPAA") and amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), part of the American Recovery and Reinvestment Act of 2009 ("ARRA"), the Genetic Information Nondiscrimination Act of 2008 ("GINA"), and the final regulations to such Acts promulgated in January 2013;

WHEREAS, to comply with the requirements of the Privacy Standards, the Covered Entity must enter into this Business Associate Agreement with the Business Associate.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter contained, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, and intending to be legally bound hereby, the parties hereto agree as follows:

I. Definitions

The following terms used in this Business Associate Agreement ("BAA") shall have the same meaning as those terms in the Privacy Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Secretary, Subcontractor, and Use. If other terms are used, but not otherwise defined under this BAA, such terms shall then have the same meaning as those terms in the Privacy Rule.

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR § 160.103.

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR § 160.103.

(c) Electronic Protected Health Information. "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 CFR §160.103.

(d) Electronic Transactions Rule. "Electronic Transactions Rule" shall mean the final regulations issued by HHS concerning standard transactions and code sets under 45 CFR Parts 160 and 162.

(e) Genetic Information. "Genetic Information" shall have the same meaning as the term "genetic information" in 45 CFR §160.103.

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

(g) Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

(h) 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.

(i) **Protected Health Information (PHI)**. “Protected Health Information (PHI)” shall have the same meaning as the term “protected health information” in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of a Covered Entity pursuant to the MSA.

(j) **Required By Law**. “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR §164.103.

(k) **Secretary**. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

(l) **Security Incident**. “Security Incident” shall have the same meaning as the term “security incident” in 45 CFR §164.304.

(m) **Security Rule**. “Security Rule” shall mean the Security Standards and Implementation Specifications at 45 CFR Part 160 and Part 164, subpart C.

(n) **Standards for Electronic Transactions Rule**. “Standards for Electronic Transactions Rule” means the final regulations issued by HHS concerning standard transactions and code sets under the Administration Simplification provisions of HIPAA, 45 CFR Part 160 and Part 162.

(o) **Subcontractor**. “Subcontractor” shall have the same meaning as the term “subcontractor” in 45 CFR §160.103.

(p) **Transaction**. “Transaction” shall have the meaning given the term “transaction” in 45 CFR §160.103

(q) **Unsecured Protected Health Information**. “Unsecured Protected Health Information” shall have the meaning given the term “unsecured protected health information” in 45 CFR §164.402.

II. Safeguarding Privacy and Security of Protected Health Information

(a) **Permitted Uses and Disclosures**. The Business Associate is permitted to use and disclose Protected Health Information that it creates or receives on the Covered Entity’s behalf or receives from the Covered Entity (or another business associate of the Covered Entity) and to request Protected Health Information on the Covered Entity’s behalf (collectively, “Covered Entity’s Protected Health Information”) only:

(i) **Functions and Activities on the Covered Entity’s Behalf**. To perform those services referred to in the MSA.

(ii) **Business Associate’s Operations**. For the Business Associate’s proper management and administration or to carry out the Business Associate’s legal responsibilities, provided that, with respect to disclosure of the Covered Entity’s Protected Health Information, either:

(A) The disclosure is Required by Law; or

(B) The Business Associate obtains reasonable assurance from any person or entity to which the Business Associate will disclose the Covered Entity’s Protected Health Information that the person or entity will:

(1) Hold the Covered Entity’s Protected Health Information in confidence and use or further disclose the Covered Entity’s Protected Health Information only for the purpose for which the Business Associate disclosed the Covered Entity’s Protected Health Information to the person or entity or as Required by Law; and

(2) Promptly notify the Business Associate (who will in turn notify the Covered Entity in accordance with the breach notification provisions) of any instance of which the person or entity becomes aware in which the confidentiality of the Covered Entity’s Protected Health Information was breached.

(C) To de-identify the information in accordance with 45 CFR § 164.514(a) – (c) as necessary to perform those services required under the MSA.

(iii) **Minimum Necessary**. The Business Associate will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of the Covered Entity’s Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that the Business Associate will not be obligated to comply with this minimum-

necessary limitation if neither the Business Associate nor the Covered Entity is required to limit its use, disclosure or request to the minimum necessary. The Business Associate and the Covered Entity acknowledge that the phrase “minimum necessary” shall be interpreted in accordance with the HITECH Act.

(b) Prohibition on Unauthorized Use or Disclosure. The Business Associate will neither use nor disclose the Covered Entity’s Protected Health Information, except as permitted or required by this BAA or in writing by the Covered Entity or as Required by Law. This BAA does not authorize the Business Associate to use or disclose the Covered Entity’s Protected Health Information in a manner that will violate Subpart E of 45 CFR Part 164 if done by the Covered Entity.

(c) Information Safeguards.

(i) Privacy of the Covered Entity’s Protected Health Information. The Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to protect the privacy of the Covered Entity’s Protected Health Information. The safeguards must reasonably protect the Covered Entity’s Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit incidental uses or disclosures made to a use or disclosure otherwise permitted by this BAA.

(ii) Security of the Covered Entity’s Electronic Protected Health Information. The Business Associate will develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that the Business Associate creates, receives, maintains, or transmits on the Covered Entity’s behalf as required by the Security Rule. The Business Associate will comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information, to prevent use or disclosure of protected health information other than as provided for by this BAA.

(iii) No Transfer of PHI Outside United States. Business Associate will not transfer Protected Health Information outside the United States without the prior written consent of the Covered Entity. In this context, a “transfer” outside the United States occurs if Business Associate’s workforce members, agents, or subcontractors physically located outside the United States are able to access, use, or disclose Protected Health Information.

(iv) Policies and Procedures. The Business Associate shall maintain written policies and procedures, conduct a risk analysis, and train and discipline its workforce.

(d) Subcontractors and Agents. In accordance with 45 CFR § 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, the Business Associate will ensure that any of its Subcontractors and agents 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.

(e) Prohibition on Sale of Records. As of the effective date specified by HHS in final regulations to be issued on this topic, the Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual unless the Covered Entity or Business Associate obtained from the individual, in accordance with 45 CFR §164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that individual, except as otherwise allowed under the HITECH Act.

(f) Prohibition on Use or Disclosure of Genetic Information. Business Associate shall not use or disclose Genetic Information for underwriting purposes in violation of the HIPAA rules.

(g) Penalties for Noncompliance. The Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the privacy rule and security rule under the HIPAA Rules, as amended by the HITECH Act.

III. Compliance with Electronic Transactions Rule

If the Business Associate conducts in whole or part Transactions on behalf of the Covered Entity for which HHS has established standards, the Business Associate will comply, and will require any Subcontractor or agent it involves with the conduct of such Transactions to comply, with each applicable requirement of the Electronic Transactions Rule. The Business Associate shall also comply with the National Provider Identifier requirements, if and to the extent applicable.

IV. Obligations of the Covered Entity

The Covered Entity shall notify the Business Associate of:

- (a) Any limitation(s) in its notice of privacy practices of the Covered Entity in accordance with 45 CFR §164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of Protected Health Information;
- (b) Any changes in, or revocation of, permission by the Individual to use or disclose Protected Health Information, to the extent that such changes may affect the Business Associate's use or disclosure of Protected Health Information; and
- (c) Any restriction to the use or disclosure of Protected Health Information that the Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of Protected Health Information.

V. Permissible Requests by the Covered Entity

The Covered Entity shall not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity.

VI. Individual Rights

(a) Access. The Business Associate will, within twenty-five (25) calendar days following the Covered Entity's request, make available to the Covered Entity or, at the Covered Entity's direction, to an individual (or the individual's personal representative) for inspection and obtaining copies of the Covered Entity's Protected Health Information about the individual that is in the Business Associate's custody or control, so that the Covered Entity may meet its access obligations under 45 CFR §164.524. Effective as of the date specified by HHS, if the Protected Health Information is held electronically in a designated record set in the Business Associate's custody or control, The Business Associate will provide an electronic copy in the form and format specified by the Covered Entity if it is readily producible in such format; if it is not readily producible in such format, the Business Associate will work with the Covered Entity to determine an alternative form and format as specified by the Covered Entity to meet its electronic access obligations under 45 CFR §164.524.

(b) Amendment. The Business Associate will, upon receipt of written notice from the Covered Entity, promptly amend or permit the Covered Entity access to amend any portion of the Covered Entity's Protected Health Information in a designated record set as directed or agreed to by the Covered Entity, so that the Covered Entity may meet its amendment obligations under 45 CFR §164.526.

(c) Disclosure Accounting. The Business Associate will maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 CFR §164.528.

(i) Disclosures Subject to Accounting. The Business Associate will record the information specified below ("Disclosure Information") for each disclosure of the Covered Entity's Protected Health Information, not excepted from disclosure accounting as specified below, that the Business Associate makes to the Covered Entity or to a third party.

(ii) Disclosures Not Subject to Accounting. The Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of the Covered Entity's Protected Health Information if the Covered Entity need not account for such disclosures under the HIPAA Rules.

(iii) Disclosure Information. With respect to any disclosure by the Business Associate of the Covered Entity's Protected Health Information that is not excepted from disclosure accounting under the HIPAA Rules, the Business Associate will record the following Disclosure Information as applicable to the type of accountable disclosure made:

(A) Disclosure Information Generally. Except for repetitive disclosures of the Covered Entity's Protected Health Information as specified below, the Disclosure Information that the Business Associate must record for each accountable disclosure is (1) the disclosure date, (2) the name and (if known) address of the entity to which the Business Associate made the disclosure, (3) a brief description of the Covered Entity's Protected Health Information disclosed, and (4) a brief statement of the purpose of the disclosure.

(B) Disclosure Information for Repetitive Disclosures. For repetitive disclosures of the Covered Entity's Protected Health Information that the Business Associate makes for a single purpose to the same person or

entity (including the Covered Entity), the Disclosure Information that the Business Associate must record is either the Disclosure Information specified above for each accountable disclosure, or (1) the Disclosure Information specified above for the first of the repetitive accountable disclosures; (2) the frequency, periodicity, or number of the repetitive accountable disclosures; and (3) the date of the last of the repetitive accountable disclosures.

(iii) Availability of Disclosure Information. The Business Associate will maintain the Disclosure Information for at least 6 years following the date of the accountable disclosure to which the Disclosure Information relates (3 years for disclosures related to an Electronic Health Record, starting with the date specified by HHS). The Business Associate will make the Disclosure Information available to the Covered Entity within twenty-five (25) calendar days following the Covered Entity's request for such Disclosure Information to comply with an individual's request for disclosure accounting. Effective as of the date specified by HHS, with respect to disclosures related to an Electronic Health Record, the Business Associate shall provide the accounting directly to an individual making such a disclosure request, if a direct response is requested by the individual. 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, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

(d) Restriction Agreements and Confidential Communications. The Covered Entity shall notify the Business Associate of any limitations in the notice of privacy practices of Covered Entity under 45 CFR §164.520, to the extent that such limitation may affect the Business Associate's use or disclosure of Protected Health Information. The Business Associate will comply with any agreement that the Covered Entity makes that either: (i) restricts use or disclosure of the Covered Entity's Protected Health Information pursuant to 45 CFR §164.522(a); or (ii) requires confidential communication about the Covered Entity's Protected Health Information pursuant to 45 CFR §164.522(b), provided that the Covered Entity notifies the Business Associate in writing of the restriction or confidential communication obligations that the Business Associate must follow. The Covered Entity will promptly notify the Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct the Business Associate whether any of the Covered Entity's Protected Health Information will remain subject to the terms of the restriction agreement. Effective February 17, 2010 (or such other date specified as the effective date by HHS), the Business Associate will comply with any restriction request if: (i) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (ii) the Protected Health Information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

VII. Breaches and Security Incidents

(a) Reporting.

(i) Impermissible Use or Disclosure. The Business Associate will report to Covered Entity any use or disclosure of Protected Health Information not permitted by this BAA not more than twenty-five (25) calendar days after Business Associate becomes aware of such non-permitted use or disclosure.

(ii) Privacy or Security Breach. The Business Associate will report to the Covered Entity any use or disclosure of the Covered Entity's Protected Health Information not permitted by this BAA of which it becomes aware, including breaches of Unsecured Protected Health Information as required by 45 CFR 164.410, and any Security Incident of which it becomes aware. The Business Associate will make the report to the Covered Entity's Privacy Official not more than twenty-five (25) calendar days after the Business Associate becomes aware of such non-permitted use or disclosure. If a delay is requested by a law-enforcement official in accordance with 45 CFR §164.412, the Business Associate may delay notifying the Covered Entity for the applicable time period. The Business Associate's report will at least:

(A) Identify the nature of the Breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of the Breach;

(B) Identify the Covered Entity's Protected Health Information that was subject to the non-permitted use or disclosure or Breach (such as whether full name, social security number, date of birth, home address, account number or other information were involved) on an individual basis;

(C) Identify who made the non-permitted use or disclosure and who received the non-permitted use or disclosure;

(D) Identify what corrective or investigational action the Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects and to protect against any further Breaches;

(E) Identify what steps the individuals who were subject to a Breach should take to protect themselves; and

(F) Provide such other information, including a written report and risk assessment under 45 CFR §164.402, as the Covered Entity may reasonably request.

(iii) Security Incidents. The Business Associate will report to The Covered Entity any Security Incident of which the Business Associate becomes aware. The Business Associate will make this report once per month, except if any such Security Incident resulted in a disclosure not permitted by this BAA or Breach of Unsecured Protected Health Information, Business Associate will make the report in accordance with the provisions set forth above.

(b) Mitigation. The Business Associate shall mitigate, to the extent practicable, any harmful effect known to the Business Associate resulting from a use or disclosure in violation of this BAA.

VIII. Term and Termination

(a) Term. The term of this BAA shall be effective as of the date specified below and shall terminate when all Protected Health Information provided by the Covered Entity to the Business Associate or created or received by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity upon termination of the MSA.

(b) Right to Terminate for Cause. The Covered Entity may terminate the MSA if it determines, in its sole discretion, that the Business Associate has breached a material term of this BAA, and upon written notice to the Business Associate of the breach, the Business Associate fails to cure the breach within thirty (30) calendar days after receipt of the notice. Any such termination will be effective immediately or at such other date specified in the Covered Entity's notice of termination.

(c) Treatment of Protected Health Information on Termination.

(i) Return or Destruction of Covered Entity's Protected Health Information as Feasible. Upon termination or other conclusion of service provided under the MSA, the Business Associate will, if feasible, return to the Covered Entity or destroy all of the Covered Entity's Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived there from that allow identification of any individual who is a subject of the Covered Entity's Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of the Business Associate. Further, the Business Associate shall require any such Subcontractor or agent to certify to the Business Associate that it returned to the Business Associate (so that the Business Associate may return it to the Covered Entity) or destroyed all such information which could be returned or destroyed. The Business Associate will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of the MSA.

(ii) Procedure When Return or Destruction Is Not Feasible. The Business Associate will identify any of the Covered Entity's Protected Health Information, including any that the Business Associate has disclosed to Subcontractors or agents as permitted under this BAA, that cannot feasibly be returned to the Covered Entity or destroyed and explain why return or destruction is infeasible. The Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. The Business Associate will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of the MSA.

(iii) Continuing Privacy and Security Obligation. The Business Associate's obligation to protect the privacy and safeguard the security of the Covered Entity's Protected Health Information as specified in this BAA will be continuous and survive termination or other conclusion of this BAA and the MSA.

IX. Miscellaneous Provisions

(a) Definitions. All terms that are used but not otherwise defined in this BAA shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance.

- (b) Inspection of Internal Practices, Books, and Records.** The Business Associate will make its internal practices, books, and records relating to its use and disclosure of the Covered Entity's Protected Health Information available to the Covered Entity and to HHS to determine compliance with the HIPAA Rules.
- (c) Amendment to Agreement.** This BAA may be amended only by a written instrument signed by the parties. In case of a change in applicable law, the parties agree to negotiate in good faith to adopt such amendments as are necessary to comply with the change in law.
- (d) No Third-Party Beneficiaries.** Nothing in this BAA shall be construed as creating any rights or benefits to any third parties.
- (e) Regulatory References.** A reference in this BAA to a section in the Privacy Rule means the section as in effect or as amended.
- (f) Survival.** The respective rights and obligations under this BAA shall survive the termination of the MSA
- (g) Interpretation.** Any ambiguity in this BAA shall be resolved to permit the Covered Entity to comply with the HIPAA Rules.
- (h) Notices.** All notices hereunder shall be in writing and delivered by hand, by certified mail, return receipt requested or by overnight delivery. Notices shall be directed to the parties at their respective addresses set forth in the first paragraph of this BAA or below their signature, as appropriate, or at such other addresses as the parties may from time to time designate in writing.
- (i) Entire Agreement; Modification.** This BAA represents the entire agreement between the Business Associate and the Covered Entity relating to the subject matter hereof. No provision of this BAA may be modified, except in writing, signed by the parties.
- (j) Indemnification.** Each Party agrees to indemnify, defend and hold harmless each other Party, its affiliates and each of their respective directors, officers, employees, agents or assigns from and against any and all actions, causes of actions, claims, suits and demands whatever, and from all damages, liabilities, costs, charges, debts and expenses whatever (including reasonable attorneys' fees and expenses related to any litigation or other defense of any claims), which may be asserted or for which they may now or hereafter become subject arising in connection with (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of the Party to the MSA or this BAA; and (ii) any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of any way connected with the Party's performance.
- (k) Assistance in Litigation or Administrative Proceedings.** The Business Associate shall make itself, and any subcontractors, employees or agents assisting the Business Associate in the performance of its obligations under this BAA, available to the Covered Entity, at no cost to the Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Covered Entity, its directors, officers, or employees based upon a claimed violation of HIPAA, the HIPAA regulations, or other laws relating to security and privacy, except where the Business Associate or its subcontractors, employees, or agents are named as an adverse party.
- (l) Binding Effect.** This BAA shall be binding upon the parties hereto and their successors and assigns. For purposes of this BAA, a signed copy delivered by facsimile or electronically shall be treated by the parties as an original of this BAA and shall be given the same force and effect.
- (m) Governing Law, Jurisdiction, and Venue.** This BAA shall be governed by the law of Michigan except to the extent preempted by federal law.
- (n) Severability.** The invalidity or unenforceability of any provisions of this BAA shall not affect the validity or enforceability of any other provision of this BAA, which shall remain in full force and effect.
- (o) Construction and Interpretation.** The section headings contained in this BAA are for reference purposes only and shall not in any way affect the meaning or interpretation of this BAA. This BAA has been negotiated by the parties at arm's-length and each of them has had an opportunity to modify the language of this BAA. Accordingly, the BAA shall be treated as having been drafted equally by the parties and the language shall be construed as a whole and according to its fair meaning. Any presumption or principle that the language is to be construed against any party shall not apply. This

BAA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

(p) *Electronic Signature.* An electronic signature captured within a software system will result in a legally binding contract under applicable state law.

In Witness Whereof, the parties hereto have caused this BAA to be executed as of the date first above written.

BUSINESS ASSOCIATE:

BASIC Benefits LLC

Signature: _____

Print Name: _____

Title: _____

Date: _____

COVERED ENTITY:

Employer: _____

Signature: _____

Print Name: _____

Title: _____

Date: _____