

ACA MARKETPLACE ENROLLMENT SOLUTIONS

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is entered into this ____ day of _____, 201_ (the "Effective Date"), by and between ACA MARKETPLACE ENROLLMENT SOLUTIONS, a division of Hallberg Commercial Insurors, Inc., a corporation of the State of Illinois (the "Covered Entity"), and _____ (the "Business Associate" (collectively, the "Parties").

RECITALS

WHEREAS, ACA Marketplace Enrollment Solutions, a division of Hallberg Commercial Insurors, Inc., is a "covered entity" that is required to comply with the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (the "Act") and its implementing regulations, including the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") and the Security Standards for the Protection of Electronic PHI (the "Security Rule"), as amended by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") and its implementing regulations, and as they may be further amended from time to time (collectively, "HIPAA");

WHEREAS, the Business Associate, in the course of providing services to the Covered Entity, may have access to certain Protected Health Information ("PHI") and may be deemed a business associate for certain purposes under HIPAA; and

WHEREAS, the Parties contemplate that the Business Associate may obtain PHI, with the Covered Entity's knowledge and consent, from certain other business associates of the Covered Entity that may possess such PHI; and

WHEREAS, the Business Associate and the Covered Entity are entering into this BAA to set forth the Business Associate's obligations as to its handling of PHI, whether such PHI was obtained from another business associate of Covered Entity or directly from the Covered Entity.

NOW, THEREFORE, for mutual consideration, the sufficiency and delivery of which is acknowledged by the Parties, and upon the premises and covenants set forth herein, the Parties agree as follows:

1. Definitions.

Terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms in the HIPAA Rules (as defined below), the HITECH Standards (as defined below) or any future regulations promulgated or guidance issued by the Secretary (as defined below) thereunder.

"Breach" shall have the same meaning as the term "breach" at 45 C.F.R. § 164.402.

"Designated Record Set" shall have the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.

“Electronic Health Record” shall mean an electronic record of health-related information on an Individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.

“Electronic PHI” shall have the same meaning as the term “electronic PHI” at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of the Covered Entity.

“HIPAA” shall mean the Health Insurance Portability and Accountability Act of 1996, as amended, and the implementation regulations thereunder, including without limitation the HIPAA Rules (as defined below) and the HITECH Standards (as defined below), and all future regulations promulgated thereunder.

“HIPAA Rules” means the Privacy Rule (as defined below) and the Security Rule (as defined below).

“HITECH Standards” means Subtitle D of the HITECH Act, found at Title XIII of the American Recovery and Reinvestment Act of 2009, and any regulations promulgated thereunder, including all amendments to the HIPAA Rules.

“Individual” shall have the same meaning as the term “individual” at 45 C.F.R. § 160.103, and any amendments thereto, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

“Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164.

“Protected Health Information” or “PHI” shall have the same meaning as the term “protected health information” at 45 C.F.R. § 160.103, and any amendments thereto, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

“Required by Law” shall have the same meaning as the term “required by law” at 45 C.F.R. § 164.103.

“Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her designee.

“Security Incident” shall have the same meaning as the term “security incident” at 45 C.F.R. § 164.304.

“Security Rule” shall mean the Security Standards for the Protection of Electronic PHI at 45 C.F.R. Parts 160, 162 and 164.

“Unsecured PHI” shall have the same meaning as the term “unsecured protected health information” at 45 C.F.R. § 164.402.

2. Obligations and Activities of Business Associate.

To the extent that the Business Associate is provided with or creates any PHI on behalf of the Covered Entity and is acting as a business associate of the Covered Entity, the Business Associate shall comply with the provisions of HIPAA applicable to business associates, and in doing so, represents and warrants as follows:

- (a) Use or Disclosure. The Business Associate shall not use or disclose PHI other than as set forth in this BAA or as Required by Law.
- (b) Minimum Necessary. The Business Associate shall make reasonable efforts, to the extent practicable, to limit requests for and the use and disclosure of PHI to a Limited Data Set (as defined in 45 C.F.R. § 164.514(e)(2)) or, if needed by the Business Associate, to the minimum necessary PHI to accomplish the intended purpose of such use, disclosure or request, and as applicable, in accordance with the regulations and guidance issued by the Secretary on what constitutes the minimum necessary for the Business Associate to perform its obligations to Covered Entity under this BAA, any underlying agreement, or as Required by Law.
- (c) Safeguards. The Business Associate shall establish appropriate safeguards, consistent with HIPAA, that are reasonable and necessary to prevent any use or disclosure of PHI not expressly authorized by this BAA and the HIPAA Rules.
 - (i) The Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI that it creates, receives, maintains or transmits on behalf of the Covered Entity.
 - (ii) The Business Associate shall comply with the applicable requirements of the Security Rule in the same manner such provisions apply to the Covered Entity.
 - (iii) The Business Associate shall provide the Covered Entity with such written documentation concerning safeguards as the Covered Entity may reasonably request from time-to-time.
- (d) Agents and Subcontractors. In accordance with 45 C.F.R. §§ 164.308(b)(2) and 164.502(e)(1)(ii), the Business Associate shall ensure that any agents, including subcontractors, that create, receive, maintain or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions and conditions that apply through this BAA to Business Associate as to such PHI, including the requirement that they agree to implement reasonable and appropriate safeguards to protect Electronic PHI that is disclosed to them by the Business Associate. To the extent permitted by law, the Business Associate shall be fully liable to the Covered Entity for any and all acts, failures or omissions of the Business Associate's agents and subcontractors in any breach of their subcontracts or assurances to the Business Associate as though they were the Business Associate's own acts, failures or omissions.

- (e) Reporting. The Business Associate shall report to the Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware.
- (i) To the extent that the Business Associate creates, receives, maintains or transmits Electronic PHI, the Business Associate shall report as soon as practicable to Covered Entity any Security Incident, as determined by the Business Associate, involving PHI of which the Business Associate becomes aware. Notwithstanding the foregoing, the Business Associate and the Covered Entity acknowledge the ongoing existence and occurrence of attempted but unsuccessful Security Incidents that are trivial in nature, such as pings and port scans, and the Covered Entity acknowledges and agrees that no additional notification to the Covered Entity of such unsuccessful Security Incidents is required.
 - (ii) To the extent that the Business Associate becomes aware of an unusually high number of such unsuccessful Security Incidents due to the repeated acts of a single party, the Business Associate shall notify the Covered Entity of these attempts and provide the name, if available, of said party.
 - (iii) At the request of the Covered Entity, the Business Associate shall identify the date of the Security Incident, the scope of the Security Incident, the Business Associate's response to the Security Incident, and the identification of the party responsible for causing the Security Incident, if known.
- (f) Notification. Following the Business Associate's discovery of a Breach of Unsecured PHI, the Business Associate shall notify the Covered Entity of the Breach without unreasonable delay, and in no event later than three (3) business days after the Business Associate, or any of its employees or agents, discovered the Breach.
- (i) Such notification shall include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used or disclosed during the Breach and any other information available to the Business Associate about the Breach which is required to be included in the notification of the Breach provided to the Individual in accordance with 45 C.F.R. § 164.404(c).
 - (ii) A Breach of Unsecured PHI shall be treated as discovered as of the first day on which such Breach is known to the Business Associate or should have been known to the Business Associate by exercising reasonable diligence.
 - (iii) If the Business Associate (or one of its subcontractors, vendors or agents) is responsible for a Breach of Unsecured PHI, the Covered Entity may, at its option, require the Business Associate to provide any of the notifications required by 45 C.F.R. § 164.404 at the Business Associate's expense.

- (g) Mitigation. The Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to the Business Associate resulting from a use or disclosure of PHI by the Business Associate in violation of the requirements of this BAA.
- (h) Audits and Inspections. The Business Associate shall make its internal practices, books and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created by the Business Associate on behalf of the Covered Entity available to the Secretary, in a time and manner mutually agreed to by the Parties or designated by the Secretary, for purposes of the Secretary determining the Covered Entity's compliance with HIPAA.
- (i) Accounting. The Business Associate shall document the Business Associate's disclosures of PHI as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. As of the compliance date set forth in the regulations promulgated under the HITECH Act or as otherwise determined by the Secretary, in addition to the accounting of disclosure obligations required under 45 C.F.R. § 164.528, the Business Associate shall account for all disclosures of PHI made through an Electronic Health Record in accordance with the HITECH Standards and any future regulations promulgated thereunder. Within ten (10) business days (or such other date that the Business Associate and the Covered Entity may reasonably agree upon) of receiving written notice from the Covered Entity that the Covered Entity has received a request for an accounting of disclosures of PHI, the Business Associate shall provide to the Covered Entity information collected to permit the Covered Entity to make the accounting required in accordance with 45 C.F.R. § 164.528.
- (j) Designated Record Set. The Business Associate shall provide access, at the request of the Covered Entity, and in a time and manner mutually acceptable to the Business Associate and the Covered Entity, to PHI in a Designated Record Set to the Covered Entity, or, as directed by the Covered Entity, to an Individual or another person properly designated by such Individual, in order to meet the requirements under 45 C.F.R. § 164.524. If the Business Associate maintains PHI of an Individual electronically in a Designated Record Set and if such Individual requests an electronic copy of such PHI, the Business Associate shall provide the Covered Entity, or such Individual or person properly designated by such Individual, as directed by the Covered Entity, access to such PHI in the electronic form and format requested by such Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Covered Entity and such Individual. Any fee that the Business Associate may charge for such electronic copy shall not be greater than the Business Associate's labor and supply costs in responding to the request. The Business Associate shall make any amendment(s) to PHI in its possession contained in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of the Covered Entity or an Individual, and in a time and manner mutually acceptable to the Business Associate and the Covered Entity.

- (k) Privacy Rule Obligations. To the extent the Business Associate is to carry out the Covered Entity's obligations under the Privacy Rule, the Business Associate shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such delegated obligation.

3. General Use and Disclosure Provisions.

Except as otherwise limited in this BAA:

- (a) The Business Associate reserves the right to use PHI for the proper management and administration of the Business Associate's duties, to carry out the legal responsibilities of the Business Associate and to provide data aggregation services to the Covered Entity.
- (b) The Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, the Covered Entity provided that such use or disclosure would not violate the Privacy Rule if done by the Covered Entity.
- (c) The Business Associate may disclose PHI in its possession for the proper management and administration of the Business Associate, provided that disclosures are Required by Law, or the Business Associate obtains reasonable assurances from the third party to whom such PHI is disclosed that such PHI will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to such third party, and such third party notifies the Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

4. Indemnification, Settlement and Procedure.

Notwithstanding any agreement by the Parties to the contrary, the Business Associate shall indemnify and hold harmless the Covered Entity and its directors, officers, affiliates, agents, volunteers, trustees or employees from and against any claim, cause of action, liability, damage, cost or expense, including attorney's fees and court or proceeding costs, arising out of or in connection with the Business Associate's material breach of its obligations under this BAA, as well as any violation of or failure of the Business Associate to fulfill its obligations under HIPAA, including the unauthorized use or disclosure of PHI, or any failure in security measures affecting PHI by the Business Associate, its subcontractors, vendors or agents, or any person or entity under the Business Associate's control. The Business Associate's obligation to indemnify the Covered Entity in accordance with this Section 4 shall survive expiration or termination of this BAA. The Covered Entity may, at its option, conduct its defense or settlement of any such action arising as described herein, and the Business Associate shall cooperate with such defense and settlement.

5. Term and Termination.

- (a) Term. This BAA shall become effective upon the Effective Date and shall continue until terminated as provided herein; provided, however, that in any event this BAA shall not terminate until all of the PHI 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, or, if it is not feasible to return or destroy such PHI, protections are extended to such information, in accordance with the termination provisions in this Section 5.

- (b) Termination upon Breach. Upon either Party's knowledge of a material breach by the other Party to this BAA, including the Recitals of this BAA, the breaching Party shall notify the non-breaching Party of such breach and the breaching party shall have fourteen (14) days from the date of notification to the non-breaching party to cure such breach. Upon the Covered Entity's knowledge of a material breach of this BAA by the Business Associate, the Covered Entity shall either:
 - (i) Provide an opportunity for the Business Associate to cure the breach or end the violation and terminate this BAA if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity; or
 - (ii) Immediately terminate this BAA if the Business Associate has breached a material term of this BAA and cure is not possible.

The Business Associate shall ensure that it maintains the termination rights in this Section 5 in any agreement it enters into with a subcontractor pursuant to Section 2(d) hereof.

- (c) Termination by Either Party. Either Party may terminate this BAA upon provision of thirty (30) days' prior written notice.
- (d) Effect of Termination.
 - (i) To the extent feasible, upon termination of this BAA for any reason, the Business Associate shall return or destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall not retain copies of such PHI. The Business Associate shall complete such return or destruction as promptly as possible and verify in writing within thirty (30) days of the termination of this BAA to the Covered Entity that such return or destruction has been completed.
 - (ii) If not feasible, the Business Associate shall provide the Covered Entity notification of the conditions that make return or destruction of such PHI not feasible. Upon determination that return or destruction of such PHI is not feasible, the Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction not feasible, for so long as the Business Associate maintains such PHI.

(e) Survival.

The obligations of the Business Associate under this Section 5 shall survive the termination of this BAA.

6. Miscellaneous.

(a) Regulatory References. A reference in this BAA to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

(b) Amendment. The Parties acknowledge that the provisions of this BAA are designed to comply with HIPAA and agree to take such action as is necessary to amend this BAA from time to time as is necessary for the Covered Entity to comply with the requirements of HIPAA. Regardless of the execution of a formal amendment of this BAA, the BAA shall be deemed amended to permit the Covered Entity and the Business Associate to comply with HIPAA.

(c) Method of Providing Notice. Any notice required to be given pursuant to the terms and provisions of this BAA shall be in writing and may be either personally delivered or sent by registered or certified mail in the United States Postal Service, return receipt requested, postage prepaid, addressed to each Party at the addresses currently in effect between the Covered Entity and the Business Associate. Any such notice shall be deemed to have been given if mailed as provided herein, as of the second day after the date mailed.

(d) Parties Bound. This BAA shall inure to the benefit of and be binding upon the Parties hereto and their respective legal representatives, successors and assigns. The Business Associate may not assign or subcontract the rights or obligations under this BAA without the express written consent of the Covered Entity. The Covered Entity may assign its rights and obligations under this BAA to any successor or affiliated entity.

(e) No Waiver. No provision of this BAA or any breach thereof shall be deemed waived unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

(f) Interpretation. Any ambiguity in this BAA shall be resolved to permit compliance with HIPAA and any related guidance.

(g) No Third-Party Rights. The terms of this BAA are not intended nor should they be construed to grant any rights, remedies, obligations, or liabilities whatsoever to parties other than the Business Associate and the Covered Entity and their respective successors or assigns.

(h) Applicable Law. To the extent not governed by federal law, this BAA shall be governed under the laws of the State of Illinois.

(i) Action by Covered Entity. The Business Associate understands and acknowledges that any disclosure or misappropriation of any PHI in violation of

this BAA will cause the Covered Entity irreparable harm, the monetary amount of which may be difficult to ascertain, and therefore agrees that the Covered Entity shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining any such further disclosure or breach and for such other relief as the Covered Entity shall deem appropriate.

- (j) Action against Covered Entity. The Business Associate shall make itself and any agents, affiliates, subsidiaries, subcontractors, or employees assisting the Business Associate in the fulfillment 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 claimed violation of HIPAA or other laws relating to security and privacy, except where the Business Associate or its agents, affiliates, subsidiaries, subcontractors, or employees are a named adverse party.

- (k) Gender. As used herein, the neuter pronoun includes the masculine and the feminine pronouns.

ACA MARKETPLACE ENROLLMENT
SOLUTIONS, a Division of Hallberg
Commercial Insurors, Inc.

BUSINESS ASSOCIATE:

By_____

Name:_____

Name:_____

Title:_____