

BUSINESS ASSOCIATE AGREEMENT BETWEEN

("COVERED ENTITY")

AND

POLESTAR BENEFITS, INC.

("BUSINESS ASSOCIATE")

I. PREAMBLE

Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, the Standards for Privacy of Individually-Identifiable Health Information, 45 CFR §164.500 *et seq.*, Covered Entity and Polestar Benefits, Inc., Business Associate, ("Polestar Benefits, Inc.") (jointly, "the Parties") wish to enter into this Agreement that addresses the requirements of the HIPAA Privacy Rule with respect to "business associates," as that term is defined in the HIPAA Privacy Rule and to incorporate the additional requirements of: (i) the HIPAA Security Standards, and the HIPAA Standards for Electronic Transactions (together with the HIPAA Privacy Rule shall be collectively referred to in this Agreement as ("the HIPAA Regulations")), and (ii) the requirements of the Health Information Technology for Economic and Clinical Health Act, a part of the American Recovery and Reinvestment Act of 2009 (the "HITECH Act") that are applicable to business associates, along with any guidance and/or regulations issued by the U.S. Department of Health and Human Services ("HHS"). Covered Entity and Polestar Benefits, Inc. agree to incorporate into this Agreement any regulations issued by HHS with respect to the HITECH Act that relate to the obligations of business associates.

Specifically, this Agreement is intended to ensure that Polestar Benefits, Inc. will establish and implement appropriate safeguards (including certain administrative requirements) for "Protected Health Information", Polestar Benefits, Inc. may create, receive, use, or disclose in connection with certain functions, activities or services (collectively "services") to be provided by Polestar Benefits, Inc. to Covered Entity. The services to be provided by Polestar Benefits, Inc. are identified in a separate agreement between the Parties entitled Administration Agreement ("AA").

The Parties acknowledge and agree that in connection with the services to be provided; Polestar Benefits, Inc. may create, receive, use or disclose Protected Health Information ("PHI"). PHI is defined as individually-identifiable health information maintained or transmitted in any form or medium, including, without limitation, all information (including demographic, medical and financial information), data, documentation, and materials that relate to: (i) the past, present or future physical or mental health or condition of an individual, including genetic information; (ii) the provision of health care to an individual; or (iii) the past, present or future payment for the provision of health care to an individual. PHI does not include health information that has been de-identified in accordance with the standards for de-identification provided for in the HIPAA Regulations.

This agreement shall replace all previous Business Associate Agreements between the parties. In connection with Polestar Benefits, Inc.'s creation, receipt, use or disclosure of PHI Polestar Benefits, Inc. and Covered Entity agree as follows:

II. DEFINITIONS

A. "*Electronic PHI*" shall mean protected health information that is transmitted or maintained in any electronic media, as this term is defined in 45 C.F.R. § 160.103.

B. "*Limited Data Set*" shall mean protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- (i) Names;
- (ii) Postal address information, other town or city, state, and ZIP code;
- (iii) Telephone numbers;
- (iv) Fax numbers;
- (v) Electronic mail addresses;
- (vi) Social Security Numbers;
- (vii) Medical record numbers;

- (viii) Health plan beneficiary numbers;
- (ix) Account numbers;
- (x) Certificate license numbers;
- (xi) Vehicle identifiers and serial numbers, including license plate numbers
- (xii) Device identifiers and serial numbers;
- (xiii) Web Universal Resource Locators (URLs);
- (xiv) Internet Protocol (IP) address numbers;
- (xv) Biometric identifiers, including finger and voice prints; and
- (xvi) Full face photographic images and any comparable images.

C. *"Protected Health Information"* or *"PHI"* shall mean information created or received by a health care provider, health plan, employer, or health care clearinghouse, that: (i) relates to the past, present, or future physical or mental health or condition of an individual, provision of health care to the individual, or the past, present, or future payment for provision of health care to the individual; (ii) identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, including genetic information; and (iii) is transmitted or maintained in an electronic medium, or in any other form or medium. The use of the term *"Protected Health Information"* or *"PHI"* in this Agreement shall mean both Electronic PHI and non-electronic PHI, unless another meaning is clearly specified.

D. *"Security Incident"* shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

E. All other terms used in this Agreement shall have the meanings set forth in the applicable definitions under the HIPAA Regulations and/or the security and privacy provisions of the HITECH Act that are applicable to business associates along with any regulations issued by HHS.

III. GENERAL TERMS

A. In the event of an inconsistency between the provisions of this Agreement and the mandatory terms of the HIPAA Regulations, as may be expressly amended from time to time by the Department of Health and Human Services (HHS) or as a result of interpretations by HHS, a court of appropriate jurisdiction, or another agency having regulatory authority over the Parties, the interpretation of HHS, such court or regulatory agency shall prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with the rules of precedence.

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

C. Except as expressly provided in the HIPAA Regulations or this Agreement, this Agreement does not create any rights in third parties.

IV. SPECIFIC REQUIREMENTS OF POLESTAR BENEFITS, INC.

A. Polestar Benefits, Inc. agrees to create, receive, use or disclose PHI only in a manner consistent with this Agreement and the HIPAA Regulations and only in connection with providing the services to Covered Entity identified in the AA entered into between the parties. Accordingly, in providing services to or for the Covered Entity, Polestar Benefits, Inc. is permitted to use and disclose PHI for "treatment, payment and healthcare operations" in accordance with the HIPAA Regulations.

B. Polestar Benefits, Inc. shall report to Covered Entity any use or disclosure of PHI that is not provided for in this Agreement.

C. Polestar Benefits, Inc. shall maintain necessary safeguards to ensure that PHI is not used or disclosed except as provided for in this Agreement

D. Additionally, under the HIPAA Regulations, Polestar Benefits, Inc. also may use or disclose PHI received by Polestar Benefits, Inc. in its capacity as a business associate to the Covered Entity if:

- the *use* relates to: (a) the proper management and administration of Polestar Benefits, Inc. to carry out legal responsibilities of Polestar Benefits, Inc., or (b) data aggregation services relating to the health care operations of the Covered Entity; or
- the *disclosure* of information received in such capacity will be made in connection with a function, responsibility, or service to be performed by Polestar Benefits, Inc., *and* such disclosure is required by law *or* Polestar Benefits, Inc. obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and the person agrees to notify Polestar Benefits, Inc. of any breaches of confidentiality.

E. Polestar Benefits, Inc.'s use, disclosure or request of PHI shall utilize a Limited Data Set if practicable. Otherwise, in performing the functions and activities as specified in the AA and this Agreement, Polestar Benefits, Inc. agrees to use or disclose only the minimum necessary PHI to accomplish the intended purpose of the use or disclosure.

F. In accordance with 45 C.F.R. § 164.524 of the HIPAA Privacy Rule and, where applicable, in accordance with the HITECH Act, Polestar Benefits, Inc. will make available to those individuals who are subjects of PHI, their PHI in Designated Record Sets by providing the PHI to Covered Entity (who then will share the PHI with the individual), by forwarding the PHI directly to the individual, or by making the PHI available to such individual at a reasonable time and at a reasonable location. Polestar Benefits, Inc. shall make such information available in an electronic format where directed by Covered Entity.

G. Polestar Benefits, Inc. shall make available the information necessary to provide an accounting of disclosures of PHI as provided for in 45 C.F.R. §164.528 of the HIPAA Privacy Rule, and where so required by the HITECH ACT and/or accompanying regulations, Polestar Benefits, Inc. shall make such information available directly to the individual. Polestar Benefits, Inc. is not required to record disclosure information or otherwise account for disclosures of PHI that this Agreement or the AA in writing permits or requires: (i) for the purpose of payment activities or health care operations (except where such recording or accounting is required by the HITECH Act, and as of the effective dates for this provision of the HITECH Act), (ii) to the individual who is the subject of the PHI disclosed, or to that individual's personal representative; (iii) to persons involved in that individual's health care or payment for health care; (iv) for notification for disaster relief purposes, (v) for national security or intelligence purposes, (vi) to law enforcement officials or correctional institutions regarding inmates (vii) pursuant to an authorization; (viii) for disclosures of certain PHI made as part of a limited data set; and (ix) for certain incidental disclosures that may occur where reasonable safeguards have been implemented.

H. Polestar Benefits, Inc. shall make available PHI for amendment and incorporate or append any amendment to PHI in accordance with 45 C.F.R. §164.526 of the HIPAA Privacy Rule.

I. If an individual submits a Request for Restriction or Request for Confidential Communications to the Polestar Benefits, Inc., Polestar Benefits, Inc. and Covered Entity agree that Polestar Benefits, Inc., on behalf of Covered Entity, will evaluate and respond to these requests according to Polestar Benefits, Inc.'s own procedures for such requests.

J. Polestar Benefits, Inc. shall make available to HHS or its agents its internal practices, books and records relating to the use and disclosure of PHI with regard to this Agreement.

K. Polestar Benefits, Inc. agrees that Covered Entity shall have the right to terminate this Agreement and seek other remedies if Polestar Benefits, Inc. violates a material term of this Agreement.

L. Polestar Benefits, Inc. shall report to Covered Entity any use or disclosure of PHI that is not provided for in this Agreement and take all reasonable action to remediate and mitigate the consequences of such disclosure or use.

Polestar Benefits, Inc. acknowledges that if it fails to remediate and mitigate or cure the consequences of disclosure, the Covered Entity will do so, and Polestar Benefits, Inc. will indemnify Covered Entity for all costs and damages associated therewith.

M. Polestar Benefits, Inc. will develop, document, implement, maintain, and use appropriate administrative, technical, and physical safeguards to preserve the integrity, confidentiality, and availability of, and to prevent non-permitted use or disclosure of, PHI created or received for or from the Covered Entity. Polestar Benefits, Inc. agrees that with respect to PHI,

these safeguards at a minimum shall meet the requirements of the HIPAA Security Standards applicable to Polestar Benefits, Inc.

N. In order to comply with HIPAA Security Standards for PHI, Polestar Benefits, Inc. agrees that it shall:

1. Implement administrative, physical, and technical safeguards consistent with (and as required by) the HIPAA Security Standards that reasonably protect the confidentiality, integrity, and availability of PHI that Polestar Benefits, Inc. creates, receives, maintains, or transmits on behalf of Covered Entity, Polestar Benefits, Inc. shall develop and implement policies and procedures that meet the Security Standards documentation requirements as required by the HITECH Act;
2. As also provided for in Section IV. R., below, ensure that any agent, including a subcontractor, to whom it provides such PHI agrees to implement reasonable and appropriate safeguards to protect it;
3. Report to Covered Entity, Security Incidents of which Polestar Benefits, Inc. becomes aware that result in the unauthorized access, use, disclosure, modification, or destruction of the Covered Entity's PHI, (hereinafter referred to as "Successful Security Incidents"). Polestar Benefits, Inc. shall report Successful Security Incidents to Covered Entity as specified in Section IV. T.;
4. For any other Security Incidents that do not result in unauthorized access, use, disclosure, modification, or destruction of Covered Entity's PHI, (including for purposes of example and not for purposes of limitation, pings on Polestar Benefits, Inc.'s firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken offline, or malware such as worms or viruses)(hereinafter "Unsuccessful Security Incidents"), Polestar Benefits, Inc. shall aggregate the data and, upon Covered Entity's written request, report to Covered Entity in accordance with the reporting requirements identified in Section IV. T.;
5. Take all commercially reasonable steps to mitigate, to the extent practicable, any harmful effect known to Polestar Benefits, Inc. resulting from a Security Incident;
6. Permit termination of this Agreement if Covered Entity determines Polestar Benefits, Inc. has violated a material term of this Agreement with respect to Polestar Benefits, Inc.'s security obligation and Polestar Benefits, Inc. is unable to cure the violation;
7. Upon Covered Entity's request, Polestar Benefits, Inc. will provide Covered Entity with access to, and copies of, documentation regarding Polestar Benefits, Inc.'s safeguards for PHI.

O. Polestar Benefits, Inc. shall conduct Standard Transactions consistent with 45 CFR Part 162 for or on behalf of Covered Entity to the extent such Standard Transactions are required in the course of Polestar Benefits, Inc.'s performing services under the AA and this Agreement for Covered Entity. As provided for in Section IV. R., below Polestar Benefits, Inc. will require any agent or subcontractor involved with the conduct of such Standard Transactions to comply with each applicable requirement of 45 CFR Part 162. Further, Polestar Benefits, Inc. will not enter into, or permit its agents or subcontractors to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that:

1. Changes the definition, data condition, or use of data element or segment in a Standard Transaction;
2. Adds any data element or segment to the maximum defined data set;
3. Uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification; or
4. Changes the meaning or intent of the Standard Transaction's implementation specification.

P. Polestar Benefits, Inc., Plan Sponsor and Covered Entity recognize and agree that communications between the parties that are required to meet the Standards for Electronic Transactions will meet the Standards set by that regulation. Communications between Plan Sponsor and Polestar Benefits, Inc. or between Plan Sponsor and the Covered Entity do not need to comply with the HIPAA Standards for Electronic Transactions. Accordingly, unless agreed to otherwise by the Parties

in writing, all communications (if any) for purposes of "enrollment" as that term is defined in 45 CFR Part 162, Subpart O or for "Health Covered Entity Premium Payment Data" as that term is defined in 45 CFR Part 162, Subpart Q, shall be conducted between the Plan Sponsor and either Polestar Benefits, Inc. or Covered Entity. For all such communications (and any other communications between Plan Sponsor and Polestar Benefits, Inc., Plan Sponsor shall use such forms, tape formats or electronic formats as Polestar Benefits, Inc. may approve. Plan Sponsor will include all information reasonably required by Polestar Benefits, Inc. to affect such data exchanges or notifications.

Q. All communications between Polestar Benefits, Inc. and Covered Entity required to meet the HIPAA Standards for Electronic Transactions shall do so. For any other communications between Polestar Benefits, Inc. and Covered Entity, Covered Entity shall use such forms, tape formats, or electronic formats as Polestar Benefits, Inc. may approve. Covered Entity shall include all information reasonably required by Polestar Benefits, Inc. to affect such data exchanges or notifications.

R. Polestar Benefits, Inc. shall include in all contracts with its agents or subcontractors, if such contracts involve disclosure of PHI to the agents or subcontractors, the same restrictions and conditions on the use, disclosure and security of such PHI as set forth in this Agreement.

S. Polestar Benefits, Inc. shall notify and report to Covered Entity (in the manner and within the timeframes described below) any use or disclosure of PHI not permitted by this Agreement, by applicable law, or permitted in writing by Covered Entity.

T. Polestar Benefits, Inc. shall notify Covered Entity following discovery and without unreasonable delay, but in no event later than twenty (20) calendar days following discovery of any "Breach" of "Unsecured Protected Health Information" as these terms are defined by the HITECH Act and its implementing regulations. Polestar Benefits, Inc. shall cooperate with Covered Entity in investigating the Breach and in meeting Covered Entity's obligations under the HITECH Act. Polestar Benefits, Inc. shall follow its notification requirements outlined immediately below:

1. For Successful Security Incidents and any other use or disclosure of PHI not permitted by the Agreement, the AA, applicable law, or without the written approval of the Covered Entity, Polestar Benefits, Inc.-without unreasonable delay and in no event later than thirty (30) days after Polestar Benefits, Inc. learns of such non permitted use or disclosure-shall provide Covered Entity a report that will:

- a. Identify (if known) each individual whose Unsecured PHI has been or is reasonably believed by Polestar Benefits, Inc. to have been accessed, acquired, or disclosed during such Breach;
- b. Identify the nature of the non-permitted access, use, or disclosure including the date of the incident and the date of discovery;
- c. Identify the PHI accessed, used, or disclosed (e.g., name, SSN, DOB);
- d. Identify who made the non-permitted access, use or received the non-permitted disclosure;
- e. Identify the corrective action Polestar Benefits, Inc. has taken or will take to prevent further non-permitted accesses, uses or disclosures;
- f. Identify what Polestar Benefits, Inc. has done or will do to mitigate any deleterious effect of the non-permitted access, use or disclosure; and
- g. Provide any other information the Covered Entity may reasonably request.

2. For Unsuccessful Security Incidents, Polestar Benefits, Inc. shall provide Covered Entity, upon its written request, a report that: (i) identifies the categories of Unsuccessful Security Incidents as described in Section IV N. 4; (ii) indicates whether Polestar Benefits, Inc. believes its current defensive security measures are adequate to address all Unsuccessful Security Incidents, given the scope and nature of such attempts; and (iii) if security measures are not adequate, the measures Polestar Benefits, Inc. will implement to address the security inadequacies.

U. In compliance with the Red Flags Rule, to the extent Polestar Benefits, Inc. performs any activities on behalf of Covered Entity in connection with one or more covered accounts, as that term is defined by 16 CFR 6812(b)(3), Polestar Benefits, Inc. shall conduct such activities in accordance with reasonable policies and procedures designated to detect, prevent and mitigate the risk of identity theft.

IV. SPECIFIC REQUIREMENTS FOR THE COVERED ENTITY

A. Covered Entity shall notify Polestar Benefits, Inc. of any limitation(s) in its Notice of Privacy Practices of Covered Entity in accordance with 45 CFR §164.520 to the extent that such limitation may affect Polestar Benefits, Inc.'s use or disclosure of PHI.

B. Covered Entity shall notify Polestar Benefits, Inc. of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Polestar Benefits, Inc.'s use or disclosure of PHI.

C. Covered Entity shall notify Polestar Benefits, Inc. of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Polestar Benefits, Inc.'s use or disclosure of PHI.

D. Covered Entity shall not request Polestar Benefits, Inc. to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by Covered Entity

E. Covered Entity agrees that Polestar Benefits, Inc. shall have the right to terminate this Agreement and seek other remedies if Covered Entity violates a material term of this Agreement.

V. MUTUAL OBLIGATIONS OF THE PARTIES

A Covered Entity and Polestar Benefits, Inc. each have a right to terminate this Agreement if the other party has engaged in a pattern of activity or practice that constitutes a material breach or violation of Polestar Benefits, Inc.'s or Covered Entity's respective obligations regarding PHI under this Agreement and, on notice of such material breach or violation from the Covered Entity or Polestar Benefits, Inc., fails to take reasonable steps to cure the material breach or end the violation.

B. If Polestar Benefits, Inc. or Covered Entity fails to cure the material breach or end the violation after the other party's notice, the Covered Entity or Polestar Benefits, Inc. (as applicable) may terminate this Addendum by providing Polestar Benefits, Inc. or the Covered Entity written notice of termination, stating the uncured material breach or violation that provides the basis for the termination and specifying the effective date of the termination. Such termination shall be effective 60 days from this termination notice.

C. Polestar Benefits, Inc.'s and Covered Entity's obligation to protect the privacy and security of the PHI it created, received, maintained, or transmitted in connection with services to be provided under the AA or this Agreement will be continuous and survive termination of the AA or this Agreement for any reason. Polestar Benefits, Inc.'s other obligations and rights, and Covered Entity's obligations and rights upon termination are those set forth in this Agreement or the AA.

VI. TERM AND TERMINATION

A. The Term of this Agreement shall be effective as of AA and shall terminate when all of the PHI provided by Covered Entity to Polestar Benefits, Inc., or created or received by Polestar Benefits, Inc. on behalf of Covered Entity, is destroyed or returned to Covered Entity 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. Effect of Termination. Upon termination of this Agreement, for any reason, Polestar Benefits, Inc. shall

1. Retain only that Protected Health Information which is necessary for Polestar Benefits, Inc. to continue its proper management and administration or to carry out its legal responsibilities;
2. Destroy or return to the Covered Entity all remaining PHI provided by the Covered Entity to Polestar Benefits, Inc., or

created or received by Polestar Benefits, Inc. on behalf of the Covered Entity.

3. Not use or disclose any PHI retained by Polestar Benefits, Inc. other than for the purposes for which such PHI was retained and subject to the same conditions set out in this Agreement, which applied prior to termination.

4. Return to the Covered Entity the PHI retained by Polestar Benefits, Inc. when it is no longer needed by Polestar Benefits, Inc. for its proper management and administration or to carry out its legal responsibilities.

This provision shall also apply to PHI that is in the possession of subcontractors or agents of Polestar Benefits, Inc.

IN WITNESS WHEREOF, the parties have caused this Business Associate Agreement to be executed on their behalf by their duly authorized representatives' signatures, effective as of the date first above written.

Employer: _____

By: _____

Name: _____

Title: _____

Date: _____