# Business Associate Agreement (BAA)

This **Business Associate Agreement** ("**Agreement**") is made and effective as of date of signing by and between Nutrition Factors, Inc. a Utah Corporation (including its affiliated entities), (collectively referred to herein as "**Covered Entity**") and the Provider Partner, (referred to herein as "**Provider Partner**" as defined below).

**Whereas**, Covered Entity provides its health and wellness web-based products and services to the Provider Partner which may involve the use or disclosure of information which meets the statutory definition of Protected Health Information (defined below) under the Health Insurance Portability and Accountability Act ("**HIPAA**").

**Whereas**, under HIPAA, Covered Entity and Provider Partner must enter into a written Provider Partner Agreement with respect to the use and disclosure of Protected Health Information.

**Therefore**, in consideration of the mutual provisions contained herein, it is agreed as follows:

## RECITALS

**A.** Provider Partner has access to certain data which includes both Protected Health Information ("**PHI**") [defined in paragraph 1(d)] and non-PHI disclosed or made available by or on behalf of Covered Entity to Provider Partner and derivatives thereof.

**B.** Covered Entity and Provider Partner are required to comply with **HIPAA,** defined in paragraph 1(b) and other laws which protect the privacy, security and confidentiality of an individual's PHI.

**C.** **HIPAA** requires Covered Entity to enter into a contract with Provider Partner containing specific requirements to protect the security and confidentiality of individual's PHI, as set forth in, but not limited to, HIPAA and contained in this Agreement.

**1.** **Definitions**. All capitalized terms not defined herein shall have the meaning ascribed to them by HIPAA (defined below), including Provider Partner, Covered Entity, Data Aggregation and Designated Record Set.

**(a)** **"Breach"** shall mean the unlawful or unauthorized access to, viewing, acquisition, use or disclosure of PHI.

**(b)** **"HIPAA"** shall mean the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-005) and the rules, guidance and regulations promulgated thereunder, as amended from time to time, including 45 Code of Federal Regulations, Parts 160 and 164.

**(c)** **"Individual"** shall have the same meaning as the term "individual" under HIPAA and shall include a person who qualifies as a personal representative.

**(d) "Protected Health Information"** (**"PHI"**) shall have the meaning given to such term under HIPAA and shall include any information, whether oral or recorded in any form or medium, limited to the information created or received by Provider Partner from or on behalf of Covered Entity (i) that relates to the past, present or future physical or mental health condition of the patient, the provision of health care to patient, or the past, present or future payment for the provision of health care to patient; and (ii) that identifies the patient or with respect to which there is a reasonable basis to believe the information can be used to identify the patient.

**(e) "Secretary"** shall mean the Secretary of the U.S. Department of Health and Human Services or her/his designee.

**(f) "Security Incident"** shall mean any accidental, malicious or natural act that: (i) Results in a Breach of any PHI or credit card information; or (ii) Adversely impacts the functionality of the Dignity Health network; or (iii) Permits unauthorized access to the Dignity Health network; or (iv) Involves the loss or loss of control of a Dignity Health owned or managed information technology resource; or (v) Involves the use of Dignity Health technology resources for illegal purposes or to launch attacks against other individuals or organizations; or (vi) Impacts the integrity of Dignity Health's files or databases including, but not limited to: (1) interface failures; (2) inadequate testing or change control procedures; or (3) other failures which result in the deletion or unauthorized changes to an electronic database. A "Security Incident" shall not include any attempted access of system operations in an information system by a Packer Internet Groper (PING) program.

**(g) "State"** shall mean the state in which the Covered Entity is located.

**(h) "Subpart E"** shall mean 45 Code of Federal Regulations, Part 164, Subpart E, which consists of Sections 164.500 et seq., as amended from time to time.

**2. Permitted Uses and Disclosures by Provider Partner**

**(a) For Covered Entity**. Except as otherwise limited in the Agreement, Provider Partner (i) shall create, maintain, transmit, access, use or disclose PHI only for the benefit of Covered Entity and to perform functions, activities, or services as specified in the Agreement, and (ii) shall not use or disclose PHI in a manner that would violate HIPAA if done by Covered Entity. Provider Partner shall only use and disclose the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure.

**(b) Minimum Necessary**. Provider Partner shall use only the minimum amount of PHI necessary to perform the specified functions, activities or services, in accordance with Covered Entity's minimum necessary policies and procedures. In the event of inadvertent access by Provider Partner to more than the minimum necessary amount of Covered Entity's PHI, Provider Partner will: (i) treat all such PHI in accordance with the Agreement; (ii) promptly notify Covered Entity, in accordance with paragraph 3(d) below, of such access; (iii) erase, delete, and/or return such PHI as quickly as possible; and (iv) take all necessary actions to prevent further unauthorized access to PHI beyond the minimum necessary amount.

**(c) Management of Provider Partner**. Except as otherwise limited in this Agreement, Provider Partner may use or disclose PHI for its proper management and administration or to carry out its legal responsibilities, provided that (i) the disclosure is required by law, or (ii) the Provider Partner obtains reasonable assurances from the person to whom the information is disclosed that such information shall remain confidential and be used or further disclosed solely as required by law or for the purpose of assisting Provider Partner to meet Provider Partner's obligations under this Agreement. Provider Partner shall require any person to whom PHI is disclosed under this subsection to notify Provider Partner of any instance of which it is aware in which the confidentiality or security of the PHI has been breached.

**(d) Data Aggregation**. Except as otherwise permitted in this Agreement, Provider Partner may use PHI to provide Data Aggregation services only for Covered Entity.

**(e) Compliance with State Laws**. Provider Partner may use, disclose and access PHI only as permitted by State law, unless such State law is contrary to HIPAA and is preempted by HIPAA in accordance with 45 Code of Federal Regulations Sections 160.201 et seq.

**3. Obligations of Provider Partner**

**(a) Use**. Provider Partner shall not use or disclose PHI other than as permitted or required by this Agreement or as required by law.

**(b) Safeguards**. Provider Partner shall use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement. Provider Partner shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, security, integrity and availability of PHI that it receives, maintains, transmits or creates on behalf of Covered Entity and that comply with the requirements of HIPAA. In addition, if Provider Partner conducts credit card transactions (i) such safeguards shall consist of or include the recommendations of the Payment Card Industry Data Security Standards, found at https://www.pcisecuritystandards.org and (ii) Provider Partner shall not store security code (i.e. CVC) information or credit card magnetic strip information in any form.

**(c) Mitigation**. Provider Partner shall promptly mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by Provider Partner in violation of this Agreement.

**(d) Notify Covered Entity**. Provider Partner shall promptly notify Covered Entity of any Security Incident or Breach in writing in the most expedient time possible, and not to exceed twenty-four (24) hours in the event of a Breach, following Provider Partner's initial awareness of such Security Incident or Breach. Notwithstanding any notice provisions in this Agreement, such notice shall be made to Nutrition Factors by email to manager@nutritionfactors.com. Provider Partner shall cooperate in good faith with Covered Entity in the investigation of any Breach or Security Incident.

**(e) Breach Notification**. Following notification to Covered Entity of a Breach, Provider Partner shall promptly cooperate with Covered Entity in determining which entity shall

provide any required Breach notification. If the parties agree that Provider Partner shall provide any required Breach notification, Provider Partner shall provide such notification timely and provide Covered Entity with documentation of Provider Partner's actions, including documentation of the names and addresses of those to whom the notifications were provided.

**(f) Access**. If Provider Partner holds PHI in Designated Record Sets as determined by Covered Entity, Provider Partner shall provide prompt access to the PHI to Covered Entity whenever so requested by Covered Entity, or, if directed by Covered Entity, to an Individual in order to meet the requirements of HIPAA and State Law, as applicable. If requested, such access shall be in electronic format. If Individual requests directly from Provider Partner (i) to inspect or copy his or her PHI, or (ii) requests its disclosure to a third party, the Provider Partner shall promptly notify Covered Entity's facility Nutrition Factors, Inc. of such request.

**(g) Amendments**. Provider Partner shall promptly make amendment(s) to PHI requested by Covered Entity and shall do so in the time and manner requested by Covered Entity to enable it to comply with HIPAA and State Law, as applicable. If Individual requests an amendment to his or her PHI, directly from Provider Partner, the Provider Partner shall promptly notify Covered Entity's facility privacy official of such request and await such official's denial or approval of the request.

**(h) Internal Records**. Provider Partner shall promptly make its internal practices, books, records, including its policies and procedures, relating to the use, disclosure, or security of PHI that the Provider Partner received from, maintained or created for or on behalf of Covered Entity, available to Covered Entity or the Secretary, in a time and manner designated by Covered Entity or the Secretary, to enable the Secretary to determine compliance with HIPAA.

**(i) Accountings**. Provider Partner shall document all disclosures of PHI and information related to such disclosures as required under HIPAA in order that it should provide an accounting of such disclosures as Covered Entity directs. Provider Partner shall: (i) Provide an accounting as required under HIPAA to those Individuals who direct their requests to Provider Partner; or (ii) Provide the accounting information required under HIPAA to Covered Entity, if so requested by Covered Entity, in the time and manner specified by Covered Entity.

**(j) Preservation**. Provider Partner shall cooperate with Covered Entity and its staff to preserve and protect the confidentiality of PHI accessed or used pursuant to this Agreement and shall not disclose or testify about such information during or after the termination of this Agreement, except as required by law.

**(k) Destruction**. If, during the term of this Agreement, Provider Partner wishes to destroy the PHI, it shall notify Covered Entity in writing about its intent to destroy data at least ten (10) business days before such date of destruction and shall comply with the requirements for destruction of PHI found in Section 5(a) of this Agreement. If Covered Entity requests the return of any PHI, Provider Partner shall comply as requested.

**(l) HIPAA Compliance**. Provider Partner shall comply with 45 Code of Federal Regulations Part 164, Subpart C with respect to electronic PHI. The written policies and

procedures and documentation required to be maintained by Provider Partner under this Agreement and HIPAA shall be made available to Covered Entity, upon Covered Entity's request.

**(m) Subcontractors**. Provider Partner shall ensure that any agent, including a subcontractor, to whom it provides PHI agrees in a written contract with Provider Partner to the same restrictions and conditions that apply to Provider Partner with respect to such information and that such agent or subcontractor shall implement reasonable and appropriate safeguards for the protection of the PHI which shall be no less than those required of Provider Partner under this Agreement and the provisions of HIPAA. In performing services under this Agreement, Provider Partner shall use agents, employees and/or subcontractors that are domiciled only within the United States of America and its territories. Notwithstanding anything to the contrary in this Agreement, Provider Partner shall not use any agent or subcontractor to perform any service requiring access to PHI under this Agreement without the express written consent of an authorized representative of Covered Entity.

**4. Effect of Breach of Obligations.** If Provider Partner breaches any of its obligations, Covered Entity shall have the option to do the following:

**(a) Cure**. Provide Provider Partner an opportunity to cure the breach, to the extent curable, and end the violation within a reasonable time specified by Covered Entity. If Provider Partner does not cure the breach or end the violation as and within the time specified by Covered Entity, or if the breach is not curable, Covered Entity may terminate its obligations to Provider Partner, including, but not limited to, its future payment obligations and obligations to provide information, materials, equipment or resources to Provider Partner; or

**(b) Termination**. Immediately terminate this Agreement, if Covered Entity reasonably determines that Provider Partner (1) has acted with gross negligence in performing its obligations; (2) is in violation of the law; (3) willfully has violated or is violating the privacy and security provisions of this Agreement or HIPAA; or (4) is unable to provide, if requested, written assurances to Covered Entity of its ability to protect the confidentiality and security of the PHI. Such termination of this Agreement shall be without prejudice to other legal remedies available to Covered Entity.

**5. Effect of Termination**

**(a) Disposition of PHI**. Upon termination of this Agreement and subject to Section 5(b) below, Provider Partner shall promptly return to Covered Entity a copy of all PHI, including derivatives thereof, and shall take all reasonable steps to promptly destroy all other PHI held by Provider Partner by: (i) shredding; (ii) securely erasing, or (iii) otherwise modifying the information in those records to make it unreadable or undecipherable through any means. This provision shall apply to PHI in the possession of subcontractors or agents of Provider Partner. At Covered Entity's request, Provider Partner shall certify in writing that it has complied with the requirements of this Section.

**(b) Infeasible; Survival**. If the return or destruction of PHI is infeasible, Provider Partner shall promptly notify Covered Entity of the conditions that make such return or

destruction infeasible. Upon mutual determination by the parties that return, or destruction of PHI is infeasible, the obligations of the Provider Partner under this Agreement shall survive the termination of this Agreement. Provider Partner shall limit the further use or disclosure of all PHI to the purposes that make its return or destruction infeasible. If Provider Partner subsequently wishes to destroy PHI, Provider Partner shall notify Covered Entity in writing about its intent to destroy data at least ten (10) business days before such date of destruction and shall comply with Section 5(a) above. If Covered Entity requests the return of any PHI, Provider Partner shall comply as requested.

**6. Credit Monitoring.** In the event that either party is required by law to notify Individuals whose PHI was inappropriately accessed, used, or disclosed by Provider Partner, its employees, subcontractor(s) or its agents, and the PHI contains: (i) the individual's first initial or first name, last name, and social security number; (ii) the individual's first initial or first name, last name, and driver's license or state identification card; (iii) the individual's first initial or first name, last name, account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; and/or (iv) the individual's first initial or first name, last name, and PHI, then Provider Partner and Covered Entity shall work together to structure a credit monitoring offering commensurate to the risk posed by the breach and Provider Partner shall, in any event, pay the costs of credit monitoring for one (1) year for such individuals and the costs and fees related to timely notification in accordance with law.

**7. Audits.** Upon reasonable notice to Provider Partner, Covered Entity shall have the right to inspect and audit Provider Partner's privacy and security protocols relating to Provider Partner's compliance with the terms of this Agreement and HIPAA. Provider Partner may impose reasonable restrictions upon Covered Entity's access to Provider Partner's premises and cloud-based information systems, including but not limited to limiting access only to those information systems which contain Covered Entity's PHI and limiting access to ensure Provider Partner's compliance with existing confidentiality obligations to its other customers. Such audits shall occur no more often than once per year or after any Breach or Security Incident and only upon a good faith belief by Covered Entity that Provider Partner is not in compliance with its obligations under this Agreement or HIPAA relating to Covered Entity's PHI. All audits shall be conducted with the least interruption to Provider Partner's normal business operations as feasible. Covered Entity shall be responsible for all costs incurred in order to perform the audit.

**8. No Third-Party Beneficiary**. The provisions and covenants set forth in this Agreement are expressly entered into only by and between Provider Partner and Covered Entity and are only for their benefit. Neither Provider Partner nor Covered Entity intends to create or establish any third-party beneficiary status or right (or the equivalent thereof) in any other third party and no such third party shall have any right to enforce or enjoy any benefit created or established by the provisions and covenants in this Agreement.

**9. Indemnity**. Provider Partner shall promptly and fully defend, indemnify, advance expenses, including, but not limited to, attorneys fees, and hold harmless Covered Entity, its affiliates and respective officers, directors, agents and employees (**"Indemnified Parties"**) against any claim, demand, liability, loss, fine, penalty, assessment, cost, judgment, award or attorney's fees (including the costs of Nutrition Factor's counsel), related to (i) the breach of

this Agreement by Provider Partner, (ii) the negligent acts or omissions of Provider Partner or any employee, subcontractor, or agent of Provider Partner, (iii) any related Breach, Security Incident or any cost of notification or remediation relating to notifications required by law, (iv) any wrongful termination or any other claim or action against Covered Entity with respect to the actual or constructive termination by Provider Partner of any agent, Provider Partner or personnel employed or contracted by Provider Partner, whether or not providing services under this Agreement and (v) any action to enforce this Section (collectively, **"Claims"**). The Claims covered by this Section shall include Claims made or recovered against the Indemnified Parties and Claims issued in favor of a third party. This Section shall survive the expiration or termination of this Exhibit.

**10. Insurance**. Provider Partner shall obtain and continuously maintain the following insurance coverages for Provider Partner and its employees, agents and independent contractors in the following amounts: (a) not less than One Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) annual aggregate of commercial general liability insurance; and (b) Two Million Dollars ($2,000,000) per occurrence and Four Million Dollars ($4,000,000) annual aggregate of errors and omissions insurance. The general liability or the errors and omissions insurance shall cover, among other things, Breaches. Provider Partner shall obtain an endorsement naming the Indemnified Parties as additional insureds. Such endorsement shall provide that the Indemnified Parties are covered for the full extent of any policy limits obtained by Provider Partner. Provider Partner shall provide Covered Entity with certificates of insurance or other written evidence of the insurance policy or policies required herein prior to the effective date of this Agreement and as of each annual renewal of such insurance policies during the term of this Agreement. Further, in the event of any modification, termination, expiration, non-renewal or cancellation of any of such insurance policies, Provider Partner shall give written notice thereof to Covered Entity not more than ten (10) business days following Provider Partner's receipt of such notification.

**11. Amendment**. The parties agree to promptly modify or amend this Agreement to permit parties to comply with any new laws, rules or regulations that might modify the terms and conditions herein.

**12. COUNTERPARTS - ELECTRONIC SIGNATURES.** This Agreement is executed in any number of counterparts such as by an electronic signature or written signature. These signatures must be treated in all respects as having the same force and effect as original signatures.

**[SIGNATURE PAGE TO FOLLOW.]**

**AGREED AND ACCEPTED:**

| **Name of Covered Entity:** | **Name of Provider Partner** |
| --- | --- |
| NUTRITION FACTORS, INCLUDING ITS AFFILIATED ENTITIES | PROVIDER PARTNER NAME, INCLUDING ITS SUBSIDIARIES, AFFILIATED ENTITIES AND SUCCESSORS IN INTEREST |
| _____<br>Authorized Signature | _____<br>Authorized Signature |
| _____<br>Print Name | _____<br>Print Name |
| _____<br>Print Title | _____<br>Print Title |
| _____<br>Date | _____<br>Date |