BUSINESS PARTNER CONTRACT/ASSOCIATE AGREEMENT

Pursuant to the privacy requirements as defined by the Health Insurance Portability and Accountability Act of 1996, Public Law No. 104-191 (HIPAA), as amended, this contract is made and entered into_____, 2013, between BenefitVision, Inc. and_____.

I. PRIVACY STANDARDS
(Compliance Date: April 14, 2003)

Both parties acknowledge that Covered Entity and Business Partner have in their possession data that contains individual identifiable health information and are in agreement that obligations necessitates the exchange of, or access to, data, and assures the privacy and confidentiality of data. Therefore, both parties agree as follows:

Definitions:

Terms used in this contract shall have the same meaning as those shown in the HIPAA Glossary.

Confidentiality:

Personally identifiable information and protected health information will be maintained in the strictest of confidence, as follows:

- Formats and encryption for transmission of electronic data are HIPAA compliant.
- Data shall not be used for any purpose other than the agreed enrollment process.
- Shall establish, maintain and use appropriate safeguards to ensure confidentiality.
- Shall enforce policies, procedures and processes of uses and disclosures to protect data and protect physical access to hardware and software during use, storage, transportation, disposition and/or destruction.
- Documentation and audits are established for all uses and disclosures of data.

Obligations of Covered Entity and Business Partner:

Without legal basis to do so, all personally identifiable information and protected health information shall not be used for any purpose other than the agreed enrollment process. All employees shall comply with the obligations set forth in this Contract and data may be accessed only by employees who need that information to perform their duties. Records will be maintained by adequate back-up procedure and shall be subject to the same extent of protection as original data.

Premises Access:

It is agreed that on-site enrollments will be conducted in a manner consistent with the restrictions set forth by Covered Entity. When given access to any premises, it is understood that everything located within the premises will be considered confidential information. Such information may be on or in a desk, PC Monitor, Laptop computer, fax machines, briefcases, filing cabinets, bins, credenzas, book cases, file folders, reports, spreadsheets, stacked paperwork, trash receptacles, recycle containers, or any other collection of data. Also, it is agreed that, except as provided by written contract, it is not permitted to verbally communicate, obtain, or copy any hard copy or electronic papers, documents, files, etc. and both parties agree to follow all written instructions related to any communications, collection, copying, maintenance, transfer, distribution and destruction of information.

Telephone and Internet:

Telephone and Internet enrollments are conducted in a manner and procedure consistent with restrictions and written instructions per contract. It is agreed that, except as provided by written contract, access to personal data or personal health information will be restricted to “minimum necessary” to administer, prepare, process or maintain the enrollment data.

Training:

Telephone, Internet, or on-site enrollments are conducted by enrollers, properly licensed, and trained on HIPAA privacy standards, as well as specifics of project.

Security:

Security procedures will ensure the protection of data and prevent the improper access to all data or transmissions. Information will be guarded appropriately, including, but not limited to, keeping information private, with proper workstation security and proper receipt, manipulation, storage, dissemination.

Enforceability and Amendments:

This contract shall be enforceable by the entities of signature and only the signatories of this contract, or their successors, may revoke, alter, change, modify, amend, or discharge this contract.

Term and Termination:

The terms of confidentiality and security shall survive the terms of the contract. Without cause, either party to this contract shall have the right to terminate this contract by giving written notice to the other party of such termination at least ninety calendar days before the effective date of such termination.

II. SECURITY STANDARDS
(Compliance Date: April 20, 2005).

The **HIPAA Security Rule** states "that the business associate will implement **administrative**, **physical** and **technical safeguards** that reasonably and appropriately protect the **confidentiality**, **integrity**, and **availability** of electronic protected health information that it **creates, receives, maintains or transmits"** on behalf of our associates.

Pursuant to the security requirements, we ensure the following:

- Electronic protected health information **has not been modified or destroyed** without authorization, and is archived until the end of required period.
- Electronic protected health information **is not made available or disclosed** to **unauthorized persons or processes.**
- **Accessibility and usability** of electronic protected health information upon **demand by an authorized person**.
- Electronic protected health information **is protected against any reasonably anticipated threats or hazards**
- Electronic protected health information **is protected against any reasonably anticipated uses or disclosures** that are not permitted by the Privacy Rule.
- Members of our **workforce are trained** in the security measures as outlined in our Security Manual. Employees have signed a statement certifying that he or she received such training, and will honor all security policies and procedures established by BenefitVision, with said statement kept in personnel file.

BenefitVision will accomplish the measures of administrative safeguards, physical safeguards, and technical safeguards, as follows:

- **Conducting assessments, evaluations, and developing plans, policies** and **procedures to protect** electronic protected health information.
- **Employing security measures to protect the physical premises** where electronic protected health information is used or stored, and **to protect tangible computer equipment** used in conjunction with electronic protected health information.
- **Employing hardware and software to safeguard** electronic protected health information.
- Properly **reporting, mitigating, or sanctioning** any **security incident**.

Our security standards are set forth in our **Security Standards Manual**. This manual is available for inspection at any of the BenefitVision, Inc. offices.

III. UPDATED PER
The American Recovery and Reinvestment Act of 2009 (ARRA) - also known as The Stimulus Bill
The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
With Varying Compliance/Effective Dates
Regarding Both the Privacy Rule and the Security Rule
as follows:

1. BenefitVision, as the Business Partner and/or Clearinghouse of Covered Entity, acknowledges that all parties now have **equal responsibility** and legal duties for both the Privacy Rule and the Security Rule, and are **equally** subject to HIPAA's sanctions for any infractions of the law. **Effective Date: February 17, 2010**

2. Should a breach occur, the Act now requires notification to each individual who is subject to a HIPAA breach, with such notices given in a timely manner, but no later than 60 days of discovery. A breach is considered to be discovered as of the first day on which the incident is known. **Effective Date: September 23, 2009/Enforcement Date: February 22, 2010**

- For breaches affecting less than 500 individuals, the law requires that a written notice be sent to each affected individual and also requires a report of such breaches be sent to the U.S. Department of Health and Human Services (HHS) annually.
- Breaches affecting more than 500 individuals require immediate notification to the U.S. Department of Health and Human Services (HHS), and require notification to the individuals via a prominent media outlet serving the state(s) and/or area.
- Such notification should contain the following information:
  - Nature of breach
  - Type of Protected Health Information (PHI)
  - Provide steps that individuals can take to protect themselves
  - Provide steps that Business Partner/Covered Entity is taking to remedy situation.
  - Provide contact information for individuals to ask questions.

Note: It is <u>not</u> a breach:

- Where an unauthorized person who receives the health information cannot reasonably have been able to retain it;
- If an unintentional acquisition, access or use occurs within the scope of employment or a professional relationship and the information does not go any further (i.e., it is not further acquired, accessed, or used or disclosed);
- If it is an inadvertent disclosure that occurs within a facility, and the information does not go any further.

3. All parties are required to comply with a request from an individual not to disclose PHI to a health plan if the PHI pertains only to an item or service the individual paid for out-of-pocket unless disclosure is otherwise required by law or for treatment.

Effective Date: February 17, 2010

4. Should the occasion arise, all parties must account for electronic disclosures made by Electronic Health Records (EHR's)

Effective Date: January 1, 2014, or

If acquired after January 1, 2009, it is effective for a disclosure made on the later of January 1, 2011, or date the provider acquires the EHR.

5. If an EHR is used, an individual has the right to obtain a copy of their PHI in electronic format. **Effective Date: January 1, 2011 or later**

6. The Act increases the civil penalties for violation of HIPAA in a tiered system, as follows: **(as updated to ARRA/HITECH per HIPAA Omnibus Rule of 2013**)

- **Did Not Know** $100-$50,000 Maximum of $1,500,000 per year
- **Reasonable Cause** $1,000-$50,000 Maximum of $1,500,000 per year
- **Willful Neglect-Corrected** $10,000-$50,000 Maximum of $1,500,000 per year
- **Willful Neglect-Not Corrected** $50,000 Maximum of $1,500,000 per year

Effective Date: September 23, 2013

NOTE: Both company and the individual employee responsible for violation are subject to fines. State Attorney Generals have authority to award damages, costs, etc. to those harmed in any way. **Effective Date: February 17, 2012**

Re "Omnibus Rule re HIPAA Modifications of 2013, please note that while BenefitVision would not normally be involved in various aspects of the new Omnibus Rule, BenefitVision, as a benefit enrollment company, will honor all modifications of this HIPAA Rule with respect to agreements as outlined in our existing contracts.

Effective March 26, 2013
Compliance Date: September 23, 2013

Signature below attests to the fact that above information has been read, understood and agrees to abide by said statement.

Ronald M. Kleiman, President
BenefitVision, Inc.

Date: _____

Signed by: _____

Printed Name: _____

Title: _____

Date: _____