

Business Associate Agreement between

_____ and Application Software, Inc.

This Agreement is made and entered into this ____ day of _____, _____, by and between _____ (“Covered Entity”) and Application Software, Inc., dba ASI and ASIFlex (“Business Associate”) (both parties collectively referred to herein as the “Parties”).

Business Associate has entered into an arrangement with Covered Entity wherein Business Associate shall provide Covered Entity with administrative services for the flexible spending accounts, including claims payment and other related services; and

Business Associate acknowledges that it is a “Business Associate” of Covered Entity as those terms are defined by the Health Insurance Portability and Accountability Act and its implementing regulations (45 C.F.R. Parts 160-164) (“HIPAA”).

In Consideration of the mutual covenants and conditions contained in this Agreement, the Parties agree as follows:

I. Definitions. Capitalized terms in this Agreement and not otherwise defined herein shall have the meanings set forth in HIPAA and the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH Act”), which definitions are hereby incorporated by reference.

- (a) *Breach.* “Breach” shall have the same meaning as the term “breach” in 45 CFR §164.402.
- (b) *Breach Notification Rule.* “Breach Notification Rule” shall mean the Standards and Implementation Specifications for Notification of Breaches of Unsecured Protected Health Information under 45 CFR Parts 160 and 164, subparts A and D.
- (c) *Business Associate.* “Business Associate” shall mean Application Software, Inc.
- (d) *Covered Entity.* “Covered Entity” shall mean _____.
- (e) *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.
- (f) *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.
- (g) *Enforcement Rule.* “Enforcement Rule” shall mean the Enforcement Provisions set forth in 45 CFR Part 160.
- (h) *Genetic Information.* “Genetic Information” shall have the same meaning as the term “genetic information” in 45 CFR §160.103.
- (i) *HHS.* “HHS” shall mean the Department of Health and Human Services.
- (j) *HIPAA Rules.* “HIPAA Rules” shall mean the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.
- (k) *HITECH Act.* “HITECH Act” shall mean the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009.

- (l) *Privacy Rule*. “Privacy Rule” shall mean the Privacy Standards and Implementation Specifications at 45 CFR Parts 160 and 164, subparts A and E.
- (m) *Protected Health Information*. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR §160.103, limited to the information created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity pursuant to this Agreement.
- (n) *Required by Law*. “Required by Law” shall have the same meaning as the term “required by law” in 45 CFR §164.103.
- (o) *Security Incident*. “Security Incident” shall have the same meaning as the term “security incident” in 45 CFR §164.304.
- (p) *Security Rule*. “Security Rule” shall mean the Security Standards and Implementation Specifications at 45 CFR Parts 160 and 164, subparts A and C.
- (q) *Subcontractor*. “Subcontractor” shall have the same meaning as the term “subcontractor” in 45 CFR §160.103.
- (r) *Transaction*. “Transaction” shall have the meaning given the term “transaction” in 45 CFR §160.103.
- (s) *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. Privacy and Security of Protected Health Information

- (a) **Permitted Uses and Disclosures.** Business Associate is permitted to use and disclose Protected Health Information only as set forth below:
 - (i) **Functions and Activities on Covered Entity’s Behalf.** To provide the following services: third party administrative services for the contracted programs.
 - (ii) **Business Associate’s Operations.** Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate or to carry out Business Associate’s legal responsibilities, provided that—
 - (A) The disclosure is Required by Law; or
 - (B) Business Associate obtains reasonable assurance from any person or entity to which Business Associate will disclose Protected Health Information that the person or entity will—
 - (1) Hold the Protected Health Information in confidence and use or further disclose the Protected Health Information only for the purpose for which Business Associate disclosed Protected Health Information to the person or entity or as Required by Law; and
 - (2) Promptly notify Business Associate of any instance of which the person or entity becomes aware in which the confidentiality of Protected Health Information was breached.
 - (iii) **Minimum Necessary.** 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 Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure, or

request, except that Business Associate will not be obligated to comply with this minimum-necessary limitation if neither Business Associate nor Covered Entity is required to limit its use, disclosure, or request to the minimum necessary under the HIPAA Rules. Business Associate and Covered Entity acknowledge that the phrase “minimum necessary” shall be interpreted in accordance with the HITECH Act and the HIPAA Rules.

(b) **Prohibition on Unauthorized Use or Disclosure.** Business Associate will neither use nor disclose Protected Health Information, except as permitted or required by this Agreement or in writing by Covered Entity or as Required by Law. This Agreement does not authorize Business Associate to use or disclose Covered Entity’s Protected Health Information in a manner that would violate the HIPAA Rules if done by Covered Entity, except as permitted for Business Associate's proper management and administration, as described above.

(c) **Information Safeguards.**

(i) **Privacy of Protected Health Information.** Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information. The safeguards must reasonably protect Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit incidental uses or disclosures made pursuant to a use or disclosure otherwise permitted by this Agreement. To the extent the parties agree that the Business Associate will carry out directly one or more of Covered Entity's obligations under the Privacy Rule, the Business Associate will comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

(ii) **Security of Covered Entity’s Electronic Protected Health Information.** Business Associate will comply with the Security Rule and will use appropriate administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on Covered Entity’s behalf.

(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.

(d) **Subcontractors.** Business Associate will require each of its Subcontractors to agree, in a written agreement with Business Associate, to comply with the provisions of the Security Rule; to appropriately safeguard Protected Health Information created, received, maintained, or transmitted on behalf of the Business Associate; and to apply the same restrictions and conditions that apply to the Business Associate with respect to such Protected Health Information.

- (e) **Prohibition on Sale of Protected Health Information.** Business Associate shall not engage in any sale (as defined in the HIPAA rules) of Protected Health Information.
- (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.** Business Associate acknowledges that it is subject to civil and criminal enforcement for failure to comply with the HIPAA Rules, to the extent provided by the HITECH Act and the HIPAA Rules.

III. Compliance with Electronic Transactions Rule. If Business Associate conducts in whole or part electronic Transactions on behalf of Covered Entity for which HHS has established standards, Business Associate will comply, and will require any Subcontractor it involves with the conduct of such Transactions to comply, with each applicable requirement of the Electronic Transactions Rule and of any operating rules adopted by HHS with respect to Transactions.

IV. Individual Rights.

- (a) **Access.** Business Associate will, within ten (10) calendar days following Covered Entity's request, make available to Covered Entity (or, at Covered Entity's written direction, to an individual or the individual's designee) for inspection and copying Protected Health Information about the individual that is in a Designated Record Set in Business Associate's custody or control, so that Covered Entity may meet its access obligations under 45 CFR §164.524. Effective September 23, 2013, if Covered Entity requests an electronic copy of Protected Health Information that is maintained electronically in a Designated Record Set in the Business Associate's custody or control, 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, Business Associate will work with Covered Entity to determine an alternative form and format that enable Covered Entity to meet its electronic access obligations under 45 CFR §164.524.
- (b) **Amendment.** Business Associate will, upon receipt of written notice from Covered Entity, promptly amend or permit Covered Entity access to amend any portion of an individual's Protected Health Information that is in a Designated Record Set in the custody or control of the Business Associate, so that Covered Entity may meet its amendment obligations under 45 CFR §164.526.
- (c) **Disclosure Accounting.** To allow Covered Entity to meet its obligations to account for disclosures of Protected Health Information under 45 CFR §164.528:
 - (i) **Disclosures Subject to Accounting.** Business Associate will record the information specified below ("Disclosure Information") for each disclosure of Protected Health Information, not excepted from disclosure accounting as specified below, that Business Associate makes to Covered Entity or to a third party.
 - (ii) **Disclosures Not Subject to Accounting.** Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of Protected Health Information if Covered Entity need not account for such disclosures under the HIPAA Rules.

- (iii) **Disclosure Information.** With respect to any disclosure by Business Associate of Protected Health Information that is not excepted from disclosure accounting under the HIPAA Rules, 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 Protected Health Information as specified below, the Disclosure Information that Business Associate must record for each accountable disclosure is (i) the disclosure date, (ii) the name and (if known) address of the entity to which Business Associate made the disclosure, (iii) a brief description of the Protected Health Information disclosed, and (iv) a brief statement of the purpose of the disclosure.
 - (B) **Disclosure Information for Repetitive Disclosures.** For repetitive disclosures of Protected Health Information that Business Associate makes for a single purpose to the same person or entity (including Covered Entity), the Disclosure Information that Business Associate must record is either the Disclosure Information specified above for each accountable disclosure, or (i) the Disclosure Information specified above for the first of the repetitive accountable disclosures; (ii) the frequency, periodicity, or number of the repetitive accountable disclosures; and (iii) the date of the last of the repetitive accountable disclosures.
- (iv) **Availability of Disclosure Information.** 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. Business Associate will make the Disclosure Information available to Covered Entity within ten (10) calendar days following Covered Entity's request for such Disclosure Information to comply with an individual's request for disclosure accounting.
- (d) **Restriction Agreements and Confidential Communications.** Covered Entity shall notify 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 Business Associate's use or disclosure of Protected Health Information. Business Associate will comply with any notice from Covered Entity to (1) restrict use or disclosure of Protected Health Information pursuant to 45 CFR §164.522(a), or (2) provide for confidential communications of Protected Health Information pursuant to 45 CFR §164.522(b), provided that Covered Entity notifies Business Associate in writing of the restriction or confidential communications obligations that Business Associate must follow. Covered Entity will promptly notify Business Associate in writing of the termination of any such restriction or confidential communications requirement and, with respect to termination of any such restriction, instruct Business Associate whether any of the Protected Health Information will remain subject to the terms of the restriction agreement.

V. Breaches and Security Incidents.

(a) Reporting.

- (i) **Impermissible Use or Disclosure.** Business Associate will report to Covered Entity any use or disclosure of Protected Health Information not permitted by this Agreement not more than ten (10) calendar days after Business Associate discovers such non-permitted use or disclosure.
- (ii) **Breach of Unsecured Protected Health Information.** Business Associate will report to Covered Entity any potential Breach of Unsecured Protected Health Information not more than ten (10) calendar days after discovery of such potential

Breach. Business Associate will treat a potential Breach as being discovered in accordance with 45 CFR §164.410. Business Associate will make the report to Covered Entity's Privacy Officer. If a delay is requested by a law-enforcement official in accordance with 45 CFR §164.412, Business Associate may delay notifying Covered Entity for the applicable time period. Business Associate's report will include at least the following, provided that absence of any information will not be cause for Business Associate to delay the report:

- (A) Identify the nature of the Breach, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of any Breach;
- (B) Identify the types of Protected Health Information that were involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, or other information were involved);
- (C) Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;
- (D) Identify what corrective or investigational action 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;
- (F) Provide such other information, including a written report and risk assessment under 45 CFR §164.402, as Covered Entity may reasonably request.

- (iii) **Security Incidents.** Business Associate will report to Covered Entity any Security Incident of which Business Associate becomes aware. Business Associate will make this report once per month, on or before the 10th calendar day of such month, except if any such Security Incident resulted in a disclosure not permitted by this Agreement or Breach of Unsecured Protected Health Information, Business Associate will make the report in accordance with the provisions set forth above. Trivial incidents that occur on a daily basis, such as scans, "pings," or unsuccessful attempts that do not penetrate computer networks or servers or result in interference with system operations will not be reported.
- (b) **Mitigation.** 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 Agreement.
- (c) **Breach Notification to Third Parties.**
 - (i) Where necessary or required by law, Business Associate agrees to provide by mail or (if specifically requested by the Individual) e-mail, written notification to each affected Individual of any Breach of Unsecured PHI not provided for by the Agreement of which it becomes aware and/or any Security Incident of which it becomes aware. If current contact information is unavailable, notice may be provided on Business Associate's website, or major print or broadcast media (i.e. newspapers or television) in the geographic areas where the affected Individuals most likely reside.
 - (ii) Where necessary or required by law, Business Associate agrees to provide notice to prominent media outlets following the discovery of any Breach of Unsecured PHI not provided for by this Agreement of which it becomes aware and/or any Security Incident of which it becomes aware in which the PHI of more than 500 Individuals residing in the State or specific jurisdiction is, or is reasonably believed to have been

accessed, acquired or disclosed during such Breach. If the Breach involves less than 500 Individuals, Business Associate agrees to maintain a log of the Breach and to submit the log to HHS annually.

VI. Term and Termination.

- (a) **Term.** This Agreement shall be effective as of this ____ day of _____, _____, and shall terminate upon the end date of the underlying services agreement, subject to the provisions regarding return or destruction of PHI.
- (b) **Right to Terminate for Cause.** Covered Entity may terminate this Agreement if it determines, in its sole discretion, that Business Associate has breached any provision of this Agreement, and after written notice to Business Associate of the breach, Business Associate has failed 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 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 Is Feasible.** Upon termination of this Agreement, Business Associate will, if feasible, return to Covered Entity or destroy all Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of the Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of any Subcontractors of Business Associate. Further, Business Associate shall require any such Subcontractor to certify to Business Associate that it has returned or destroyed all such information which could be returned or destroyed. Business Associate will complete these obligations as promptly as possible, but not later than ten (10) calendar days following the effective date of the termination of this Agreement.
 - (ii) **Procedure When Return or Destruction Is Not Feasible.** Business Associate will identify any Protected Health Information, including any Protected Health Information that Business Associate has disclosed to Subcontractors, that cannot feasibly be returned to Covered Entity or destroyed and explain why return or destruction is infeasible. Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. Business Associate will complete these obligations as promptly as possible, but not later than sixty (60) calendar days following the effective date of the termination or other conclusion of Agreement.
 - (iii) **Continuing Privacy and Security Obligation.** Business Associate's obligation to protect the privacy and safeguard the security of Protected Health Information as specified in this Agreement will be continuous and survive termination or other conclusion of this Agreement.

VII. General Provisions.

- (a) **Definitions.** All terms that are used but not otherwise defined in this Agreement shall have the meaning specified under HIPAA, including its statute, regulations, and other official government guidance.
- (b) **Inspection of Internal Practices, Books, and Records.** Business Associate will make its internal practices, books, and records relating to its use and disclosure of Protected

Health Information available to Covered Entity and to HHS to determine compliance with the HIPAA Rules.

- (c) **Amendment to Agreement.** This Agreement 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 Agreement shall be construed as creating any rights or benefits to any third parties.
- (e) **Interpretation.** Any ambiguity in the Agreement shall be resolved to permit Covered Entity and Business Associate to comply with the applicable requirements under the HIPAA Rules.
- (f) **Governing Law, Jurisdiction, and Venue.** This Agreement shall be governed by the law of _____, except to the extent preempted by federal law.
- (g) **Severability.** The invalidity or unenforceability of any provisions of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect.
- (h) **Construction and Interpretation.** The section headings contained in this Agreement are for reference purposes only and shall not in any way affect the meaning or interpretation of this Agreement. This Agreement has been negotiated by the parties at arm's-length and each of them has had an opportunity to modify the language of the Agreement. Accordingly, the Agreement 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 Agreement 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.
- (i) **Notices.** All notices and communications required by this Agreement shall be in writing. Such notices and communications shall be given in one of the following forms: (i) by delivery in person, (ii) by a nationally-recognized, next-day courier service, (iii) by first-class, registered or certified mail, postage prepaid; or (iv) by electronic mail to the address that each party specifies in writing.
- (j) **Entire Agreement.** This Agreement constitutes the entire agreement between the parties with respect to its subject matter and constitutes and supersedes all prior agreements, representations and understandings of the parties, written or oral, with regard to this same subject matter.

The Parties hereto execute this Agreement the date indicated above.

Application Software, Inc.

By: _____

By: _____

Title: _____

Title: _____