

	<b>State of South Carolina</b>  <b>Request for Proposal Amendment #3</b>	Solicitation Number:	PEBA0012015
		Date Issued:	02/13/2015
		Procurement Officer:	Georgia Gillens, CPPO, CPPB
		Phone:	(803) 734-0010
		E-Mail Address:	GGillens@peba.sc.gov

DESCRIPTION: **Pharmacy Benefits Management Services**

USING GOVERNMENTAL UNIT: **S.C. Public Employee Benefit Authority (PEBA)**

*The Term "Offer" Means Your "Bid" or "Proposal". Unless submitted on-line, your offer must be submitted in a sealed package. Solicitation Number & Opening Date must appear on package exterior. See "Submitting Your Offer" provision.*

**SUBMIT YOUR OFFER by the appropriate date and time below and following the instructions on Page 3.**

SUBMIT OFFER BY (Opening Date/Time): **03/02/2014 2:30 PM E.S.T.** (See "Deadline For Submission Of Offer" provision)

QUESTIONS MUST BE RECEIVED BY: **Deadline has passed.** (See "Questions From Offerors" provision)

**NUMBER OF COPIES TO BE SUBMITTED: See Page 3. If no redacted copy is being provided, initial here \_\_\_\_\_**

CONFERENCE TYPE: <b>Mandatory meeting held previously.</b> DATE & TIME: <b>01/29/2015 10:00 AM</b>  <small>(As appropriate, see "Conferences - Pre-Bid/Proposal" &amp; "Site Visit" provisions)</small>	LOCATION: _____
--	-----------------

<b>AWARD &amp; AMENDMENTS</b>	Award will be posted on <b>03/17/2015</b> . The award, this solicitation, any amendments, and any related notices will be posted at the following web address: <a href="http://www.procurement.sc.gov">http://www.procurement.sc.gov</a>
-------------------------------	--

Unless submitted on-line, you must submit a signed copy of this form with Your Offer. By submitting a bid or proposal, You agree to be bound by the terms of the Solicitation. You agree to hold Your Offer open for a minimum of thirty (30) calendar days after the Opening Date. (See "Signing Your Offer" and "Electronic Signature" provisions.)

NAME OF OFFEROR  <small>(full legal name of business submitting the offer)</small>		Any award issued will be issued to, and the contract will be formed with, the entity identified as the Offeror. The entity named as the Offeror must be a single and distinct legal entity. Do not use the name of a branch office or a division of a larger entity if the branch or division is not a separate legal entity, i.e., a separate corporation, partnership, sole proprietorship, etc.	
AUTHORIZED SIGNATURE  <small>(Person must be authorized to submit binding offer to contract on behalf of Offeror.)</small>		TAXPAYER IDENTIFICATION NO.  <small>(See "Taxpayer Identification Number" provision)</small>	
TITLE  <small>(business title of person signing above)</small>		STATE VENDOR NO.  <small>(Register to Obtain S.C. Vendor No. at www.procurement.sc.gov)</small>	
PRINTED NAME  <small>(printed name of person signing above)</small>	DATE SIGNED	STATE OF INCORPORATION  <small>(If you are a corporation, identify the state of incorporation.)</small>	
OFFEROR'S TYPE OF ENTITY: (Check one) <span style="float: right;"><small>(See "Signing Your Offer" provision.)</small></span> <input type="checkbox"/> Sole Proprietorship <input type="checkbox"/> Partnership <input type="checkbox"/> Other			

Corporate entity (not tax-exempt)     Corporation (tax-exempt)     Government entity (federal, state, or local)

**PAGE TWO**

**(Return Page Two with Your Offer)**

<b>HOME OFFICE ADDRESS</b> (Address for offeror's home office / principal place of business)	<b>NOTICE ADDRESS</b> (Address to which all procurement and contract related notices should be sent.) (See "Notice" clause)
	_____ Area Code - Number - Extension                      Facsimile _____ E- mail Address

<b>PAYMENT ADDRESS</b> (Address to which payments will be sent.) (See "Payment" clause)	<b>ORDER ADDRESS</b> (Address to which purchase orders will be sent) (See "Purchase Orders and "Contract Documents" clauses)
_____ Payment Address same as Home Office Address _____ Payment Address same as Notice Address <b>(check only one)</b>	_____ Order Address same as Home Office Address _____ Order Address same as Notice Address <b>(check only one)</b>

**ACKNOWLEDGMENT OF AMENDMENTS**  
 Offerors acknowledges receipt of amendments by indicating amendment number and its date of issue. (See "Amendments to Solicitation" Provision)

Amendment No.	Amendment Issue Date	Amendment No.	Amendment Issue Date	Amendment No.	Amendment Issue Date	Amendment No.	Amendment Issue Date

<b>DISCOUNT FOR PROMPT PAYMENT</b> (See "Discount for Prompt Payment" clause)	10 Calendar Days (%)	20 Calendar Days (%)	30 Calendar Days (%)	_____ Calendar Days (%)
--	----------------------	----------------------	----------------------	-------------------------

**PREFERENCES - A NOTICE TO VENDORS (SEP. 2009):** On June 16, 2009, the South Carolina General Assembly rewrote the law governing preferences available to in-state vendors, vendors using in-state subcontractors, and vendors selling in-state or US end products. This law appears in Section 11-35-1524 of the South Carolina Code of Laws. A summary of the new preferences is available at [www.procurement.sc.gov/preferences](http://www.procurement.sc.gov/preferences). ***ALL THE PREFERENCES MUST BE CLAIMED AND ARE APPLIED BY LINE ITEM, REGARDLESS OF WHETHER AWARD IS MADE BY ITEM OR LOT. VENDORS ARE CAUTIONED TO CAREFULLY REVIEW THE STATUTE BEFORE CLAIMING ANY PREFERENCES. THE REQUIREMENTS TO QUALIFY HAVE CHANGED. IF YOU REQUEST A PREFERENCE, YOU ARE CERTIFYING THAT YOUR OFFER QUALIFIES FOR THE PREFERENCE YOU'VE CLAIMED. IMPROPERLY REQUESTING A PREFERENCE CAN HAVE SERIOUS CONSEQUENCES.*** [11-35-1524(E)(4)&(6)] **PREFERENCES DO NOT APPLY.**

**PREFERENCES - ADDRESS AND PHONE OF IN-STATE OFFICE:** Please provide the address and phone number for your in-state office in the space provided below. An in-state office is necessary to claim either the Resident Vendor Preference (11-35-1524(C)(1)(i)&(ii)) or the Resident Contractor Preference (11-35-1524(C)(1)(iii)). Accordingly, you must provide this information to qualify for the preference. An in-state office is not required, but can be beneficial, if you are claiming the Resident Subcontractor Preference (11-35-1524(D)). **PREFERENCES DO NOT APPLY.**

\_\_\_\_\_ In-State Office Address same as Home Office Address  
 \_\_\_\_\_ In-State Office Address same as Notice Address    **(check only one)**

IMPORTANT NOTICE

**AMENDMENT #3  
INVITATION FOR BID – PEBA0012015**

**Pharmacy Benefits Management Services**

**PLEASE NOTE:** The original Invitation for Bid Solicitation document and Amendment 1 were superseded and were replaced in their entirety by Amendment 2. Amendment #3 captures only those changes made to Amendment #2 and will form the contract along with Amendment #2. It is recommended that Offerors, discard all superseded documents as described above and refer and respond only to the solicitation as described in Amendments 2 and 3 and the most recent Excel Documents for the Technical and Financial Proposals (the Financial Proposal did not change). The latest changes to the RFP have been incorporated into Amendment 3. The follow-up questions and answers submitted in writing by the deadline are included as an attachment for information only. Only the changes incorporated in Amendment 3 are relevant to RFP.

**AMENDMENTS TO SOLICITATION (JAN 2004)**

(a) The Solicitation may be amended at any time prior to opening. All actual and prospective Offeror's should monitor the following web site for the issuance of Amendments: [www.procurement.sc.gov](http://www.procurement.sc.gov) (b) Offeror's shall acknowledge receipt of any amendment to this solicitation (1) by signing and returning the amendment, (2) by identifying the amendment number and date in the space provided for this purpose on Page Two, (3) by letter, or (4) by submitting a bid that indicates in some way that the bidder received the amendment. (c) If this solicitation is amended, then all terms and conditions which are not modified remain unchanged. [02-2A005-1]

## Solicitation # PEBA0012015 has been amended as follows:

Page 70, replace clause entitled “INFORMATION SECURITY – DATA LOCATION” with the following:

### INFORMATION SECURITY – DATA LOCATION

Contractor is prohibited from accessing, processing, transmitting, or storing government information, as defined in the clause titled Information Security, outside the United States. This obligation is a material requirement of this contract. [07-7B106-1]

Page 70, replace clause entitled “INFORMATION USE AND DISCLOSURE” with the following:

### INFORMATION USE AND DISCLOSURE

Except to the extent necessary for performance of the work, citizens should not be required to share information with those engaged by the government in order to access services provided by the government and such information should be used by those engaged by the government only to the extent necessary to perform the work acquired; accordingly, this clause addresses basic requirements for the Contractor’s use and disclosure of government information, which expressly includes, but is not limited to, information provided by or obtained from the citizens. Anonymizing information does not resolve the foregoing concern. This clause should be broadly interpreted to effectuate this intent. Absent express reference to this clause, this clause supersedes any other clause to the extent of any inconsistency unless and to the extent the other clause provides greater protection for government information.

(a) *Definitions.* The following terms shall have the meanings set out in the clause titled Information Security: “**compromise,**” “**government information,**” “**information,**” “**public information,**” “**software,**” “**third party,**” “**unrestricted information,**” and “**web-based service.**”

(b) *Legal mandates.* Contractor shall be permitted to use, disclose, or retain government information to the limited extent necessary to comply with any requirement imposed on Contractor by law. If it is necessary for Contractor to use, disclose, or retain government information in order to comply with a law, Contractor shall provide using governmental unit with written notice, including a description of the circumstances and applicable law, in advance of such use, disclosure or retention except to the extent prohibited by law.

(c) *Flow down.* Any reference in this clause to Contractor also includes any subcontractor at any tier. Contractor is responsible for, and shall impose by agreement the limitations and restrictions of this clause on, any other person or entity that contractor authorizes to take action related to government information.

(d) *Collecting Information.* Contractor must gather and maintain government information only to the minimum extent necessary to accomplish the work.

(e) *Rights, Disclosure and Use.* Except as otherwise expressly provided in this solicitation, Contractor agrees NOT to either (1) use or disclose government information, or (2) retain government information after termination or expiration of this contract. Contractor acquires no rights in any government information except the limited rights to use, disclose and retain the government information in accordance with the terms of this solicitation. To the extent reasonably necessary to perform the work, Contractor may: (i) disclose government information to persons having a need-to-know (e.g., subcontractors); and (ii) use (including access, process, transmit, and store) and maintain the government information itself. Before disclosing government information to a subcontractor or third party, Contractor shall give the using governmental unit detailed written notice regarding the reason for disclosure and the identity and location of the recipient. The notice shall be provided no later than fifteen (15) business days in advance of the disclosure.

(f) *Return.* Notwithstanding the using governmental unit’s failure to perform or the pendency of a dispute, Contractor agrees to promptly destroy and return to the using governmental unit all government information in its possession upon written request of using governmental unit (provided that, if the contract has not expired or been terminated, Contractor shall be excused from the performance of any work reasonably dependent on Contractor’s further access to such government information) **to the extent such request complies with any other legal or contractual obligations imposed by this contract or the law.**

(g) *Privacy Policy & Applicable Laws.* Without limiting any other legal or contractual obligations imposed by this contract or the law, Contractor shall (a) comply with its own privacy policies and written privacy statements relevant to the work, and (b) comply with (1) all laws applicable to Contractor regarding government information, and (2) all laws and standards identified in the clause entitled Information Use and Disclosure – Standards.

(h) *Safeguarding Information.* Without limiting any other legal or contractual obligations, Contractor agrees to implement and maintain reasonable and appropriate administrative, physical, and technical safeguards (including without limitation written policies and procedures) for protection of the security, confidentiality, and integrity of the government information in its possession. Upon request by using governmental unit, Contractor shall confirm Contractor’s compliance with this section in writing signed by Contractor’s most senior executive responsible for information technology security.

(i) *Actions Following Disclosure.* Immediately upon discovery of a compromise or improper use of government information, Contractor shall take such action as may be necessary to preserve forensic evidence and eliminate the cause of the compromise or improper use. As soon as practicable, but no later than twenty-four hours after discovery, Contractor shall notify using governmental unit of the compromise or improper use, including a description of the circumstances of the use or compromise. As soon as practicable after discovery, Contractor shall undertake a thorough forensic investigation of any compromise or improper use and provide the using governmental unit all information necessary to enable the using governmental

unit to fully understand the nature and extent of the compromise or improper use. With regard to any compromise or improper use of government information, Contractor shall: (1) provide any notification to third parties legally required to be provided to such parties by Contractor, and if not (e.g., if legally required of the using governmental unit), Contractor shall reimburse using governmental unit for the cost of providing such notifications; (2) pay all costs and expenses for at least two years of identity theft monitoring services (including without limitation, credit monitoring) and identity theft restoration services for any such affected individuals receiving notice where such services are appropriate given the circumstances of the incident and the nature of the information compromised; (3) pay any related fines or penalties imposed on the using governmental unit by a government authority, and (4) reimburse the Using Governmental Unit all costs reasonably incurred for communications and public relations services involved in responding to the compromise or improper use.

(j) *Survival & Remedy*. All the obligations imposed by this paragraph are material. The obligations of this section shall survive termination or expiration of the contract. Without limiting any rights the using governmental unit may have, and notwithstanding any other term of this contract, Contractor agrees that using governmental unit may have no adequate remedy at law for a breach of Contractor's obligations under this clause and therefore the using governmental unit shall be entitled to pursue equitable remedies in the event of a breach of this clause. [07-7B108-1]

**All other Terms and Conditions remain unchanged.**

**Attachment 11: Follow-up Questions & Answers is listed for your information.**

**Attachment Two (2)**  
**Business Associate Contract**

THIS AGREEMENT is entered into as of the \_\_\_ day of \_\_\_\_\_, \_\_\_\_\_ between **NAME, ADDRESS** (hereinafter referred to as “Business Associate”) and the South Carolina Public Employee Benefit Authority, 202 Arbor Lake Drive, Columbia, South Carolina 29223 (hereinafter referred to as the “Covered Entity”).

WHEREAS, the Privacy Rule (as defined below) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) permits group health plans to disclose certain Protected Health Information of a patient to a Business Associate of such plan who performs certain functions or activities on behalf of the plan, provided that the plan enters into an agreement with the Business Associate that limits the use and disclosure of such Protected Health Information to the same extent that such limitations apply to the group health plan;

WHEREAS, the Security Rule (as defined below) established national standards to protect individuals’ electronic personal health information; and

WHEREAS, the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), pursuant to Title XIII of Division A and Title IV of Division B, called the “Health Information Technology for Economic and Clinical Health” (“HITECH Act”), provides modifications to the HIPAA Security and Privacy Rule (hereinafter, all references to the “HIPAA Security and Privacy Rule” are deemed to include all amendments to such rule contained in the HITECH Act and any accompanying regulations, and any other subsequently adopted amendments or regulations); and

WHEREAS, Covered Entity is a self-funded group health plan, and Business Associate provides such functions or activities on behalf of the Covered Entity as to constitute a “Business Associate” of the Covered Entity, as defined in the Privacy Rule;

WHEREAS, Covered Entity and Business Associate have heretofore entered into a separate Service Agreement;

WHEREAS, Covered Entity and Business Associate do hereby desire to enter into this Agreement as required under the Security and Privacy Rule and the provisions of the HITECH Act;

NOW, THEREFORE, for the reasons set forth above, and in consideration of the mutual promises and agreements set forth herein, Covered Entity and Business Associate do hereby contract and agree as follows:

**1. DEFINITIONS**

- (a) “Business Associate” shall mean **NAME**.
- (b) “Compliance Date” shall have the same meaning as the term “Compliance Date” in 45 CFR § 160.103.
- (c) “Covered Entity” shall mean the South Carolina Public Employee Benefit Authority.
- (d) “Data Aggregation” shall have the same meaning as the term “Data Aggregation” in 45 CFR § 164.501.
- (e) “Designated Record Set” shall have the same meaning as the term “Designated Record Set” in 45 CFR § 164.501.
- (f) “Electronic Protected Health Information” shall have the same meaning as “Electronic Protected Health

Information” in 45 CFR §160.103. “HITECH Act” shall have the same meaning as the Health Information Technology for Economic and Clinical Health Act, as incorporated into the American Recovery and Reinvestment Act of 2009.

- (g) “Individual” shall have the same meaning as the term “Individual” in 45 CFR §164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
- (h) “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and 164, subparts A and E.
- (i) “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” in 45 CFR § 160.103, limited to the information created or received by Business Associate from, or on behalf of, Covered Entity.
- (j) “Required By Law” shall have the same meaning as the term “Required By Law” in 45 CFR § 164.103.
- (k) “Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her designee.
- (l) “Security Incident” shall have the same meaning as “Security Incident” in 45 CFR § 164.304.
- (m) “Security Rule” shall mean the Security Standards and Implementation Specifications at 45 CFR Part 160 and 164, Subpart C.
- (n) “Service Agreement” shall mean the agreement between **NAME** and the South Carolina Public Employee Benefit Authority, whereby **NAME** performs plan management and plan administrative tasks on behalf of the benefit program described herein as Covered Entity.
- (o) “Standards for Electronic Transactions Rule” means the final regulations issued by the Department of Health and Human Services concerning standard transactions and code sets under the Administration Simplification provisions of HIPAA, 45 CFR Part 160 and Part 162.

## **2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE**

- (a) Business Associate agrees to use or disclose PHI only as permitted or required by this Agreement or as Required By Law. Business Associate is permitted to use and disclose PHI or Electronic PHI that it creates for, or receives from, Covered Entity or business associate of Covered Entity and to request PHI on behalf of Covered Entity as described in the Agreement, consistent with the HIPAA Privacy and Security Rules. When requesting, using, or disclosing PHI, Business Associate shall restrict the request, use, or disclosure of said PHI to the minimum necessary to accomplish the intended purpose of the request, use, or disclosure **in accordance with, and subject to the exceptions in, 45 CFR 164.502(b).**
- (b) Business Associate agrees to provide access to Covered Entity, at the request of Covered Entity, to PHI in a Designated Record Set in order to meet the requirements under 45 CFR § 164.524.
- (c) Business Associate agrees to make available PHI for amendment and incorporate any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity, within thirty (30) days of a written request by Covered Entity.

(d) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by, Business Associate on behalf of Covered Entity available to the Covered Entity or the Secretary, within thirty (30) days of a written request by the Covered Entity or the Secretary, for the purpose of permitting the Secretary to determine Covered Entity's compliance with the HIPAA Privacy and Security Rules.

(e) Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528 and to make available to Covered Entity, within thirty (30) days of a written request by Covered Entity, the information required to provide such an accounting to an individual. Business Associate will comply with mandates regarding individuals' rights under the HITECH Act, including rights to access and accounting of disclosures. Such information shall be made available in an electronic format where directed by Covered Entity. In addition, Business Associate shall include, within its accounting, disclosures for payment and health care operations purposes where such recording or accounting is required by the HITECH Act and as of the effective date for this provision of the HITECH Act. Covered Entity shall provide any additional information to the extent required by the HITECH Act and any accompanying regulations.

(f) Business Associate shall make information available directly to an individual within thirty (30) days, when that individual so requests, if such information is required to be disclosed under the HITECH Act and/or accompanying regulations.

(g) Business Associate agrees to develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Covered Entity's electronic and paper PHI that Business Associate creates, receives, maintains, or transmits on Covered Entity's behalf, as required by the HIPAA Security Rule and as required by the HITECH Act. Business Associate shall also develop and implement policies and procedures and meet the HIPAA Security Rule documentation requirements as required by the HITECH Act.

(h) Business Associate agrees to ensure that any agent, including a subcontractor, to whom Business Associate provides PHI, agrees to abide by the same restrictions and conditions that apply to Business Associate with respect to PHI in conformance with the Privacy Rule, and to implement reasonable and appropriate safeguards to protect it.

(i) Business Associate agrees to notify Covered Entity within two (2) business days of becoming aware of any use or disclosure of PHI not provided for by the Agreement, and within **twenty-four (24) hours** minutes of any security incident resulting in the successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system, or resulting in any "Breach" of "Unsecured Protected Health Information," as these terms are defined by the HITECH Act and any implementing regulations.

(j) Business Associate agrees to mitigate, to the extent practicable, any harmful effect it knows to have resulted from said Breach. Any such report shall include, to the extent possible, the identification (if known) of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Breach, along with any other information required to be reported under the HITECH Act and any accompanying regulations.

(k) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

(l) Business Associate agrees to maintain appropriate clearance procedures and provide supervision to ensure that its workforce follows Business Associate's security procedures.



(m) Business Associate agrees to provide appropriate training for its staff to ensure that its staff complies with its privacy and security policies.

(n) Business Associate agrees to implement appropriate security incident procedures and provide training to its applicable staff sufficient to detect and analyze security incidents.

(o) Business Associate agrees to maintain a current contingency plan in case of an emergency.

(p) Business Associate agrees, as appropriate, to maintain an emergency access plan to ensure that the PHI it holds on behalf of Covered Entity is available when needed.

(q) Business Associate agrees to implement appropriate storage, disposal and reuse procedures to protect any PHI that Business Associate holds for Covered Entity.

(r) Business Associate agrees to provide appropriate backup of the PHI that Business Associate holds for Covered Entity.

(s) Business Associate agrees to have in place appropriate authentication and access controls to safeguard the PHI that Business Associate holds for Covered Entity.

(t) Business Associate agrees to make use of encryption, as appropriate, when transmitting PHI over the Internet.

(u) Business Associate agrees to retain the documentation required by this agreement for six years from the date of its creation or the date when it last was in effect, whichever is later.

Covered Entity and Business Associate recognize and agree that in some instances **NAME** may have compliance obligations as a Health Care Provider under the Privacy Rule and nothing herein shall prohibit, restrict, or otherwise limit compliance with any such obligations by **NAME** under the Privacy Rule.

### **3. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION BY BUSINESS ASSOCIATE**

(a) Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities or services for, or on behalf of, Covered Entity, as specified in the Service Agreement, provided that such use or disclosure would not violate the Privacy and Security Rules if done by Covered Entity.

(b) Except as otherwise limited in this agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(c) Except as otherwise limited in this agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate if the disclosures are Required By Law; or if Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the PHI will remain confidential and will be used or further disclosed only as Required By Law or only for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(d) Except as otherwise limited in this agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

(e) Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).

(f) Business Associate may also use and disclose PHI: (i) to respond to requests for PHI either accompanied by an authorization that meets the requirements of 45 CFR 164.508 or from a covered entity or health care provider in accordance with 45 CFR 164.506(c); (ii) to de-identify the information or create a limited data set in accordance with 45 CFR §164.514, which de-identified information or limited data set may be used and disclosed by Business Associate as permitted by law, including HIPAA; and (iii) as authorized in writing by Covered Entity

#### **4. OBLIGATIONS OF COVERED ENTITY**

(a) Covered Entity shall notify Business Associate of any limitations in its notice(s) of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitations may affect Business Associate's use or disclosure of PHI.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity shall notify Business Associate 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 Business Associate's use or disclosure of PHI.

#### **5. PERMISSIBLE REQUESTS BY COVERED ENTITY**

Covered Entity shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under the Security and Privacy Rules if done by Covered Entity, except Business Associate may use or disclose PHI for data aggregation or management and administrative activities of Business Associate.

#### **6. TERM AND TERMINATION**

(a) Ter  
m.

The Term of this Agreement and the obligations herein shall be deemed effective as of the Compliance Date or the date of execution of this Agreement, whichever date is later, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or if it is not feasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination for Cause.

Upon either Party's (the Non-Breaching Party's) knowledge of a material breach by the other party (the Breaching Party), the Non-Breaching Party may:

(1) Provide an opportunity for the Breaching Party to cure the material breach or end the violation and terminate this Agreement if the Breaching Party does not cure the material breach or end the violation within the reasonable time specified by the Non-Breaching Party; or

(2) If neither termination nor cure is feasible, the Non-Breaching Party may report the violation to the Secretary. Failure by the Non-Breaching Party to exercise its rights to terminate under this provision shall not be construed as a waiver of its rights to terminate, rescind or revoke the services herein in case of any subsequent breach.

(c) Effect \_\_\_\_\_ of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

(2) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible, including the need to retain PHI for audit, justification of work product or compliance with other applicable law. Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI

## 7. MISCELLANEOUS

(a) Definitions. All terms that are used but not otherwise defined in this Supplement shall have the meaning specified under HIPAA, including its statute, regulations, and other official government guidance.

(b) Independent Contractor. The relationship between the parties will solely be that of independent contractors engaged in the operation of their own respective businesses.

(c) Third Party Beneficiaries. The parties agree that there are no intended third party beneficiaries under this Agreement.

(d) Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect, or as amended, and for which compliance is required.

(e) Amendment. The parties agree to take such action as is necessary to amend this Agreement as is necessary to comply with the requirements of HIPAA and other applicable law or regulation.

(f) Survival. The respective rights and obligations of Business Associate under Section 6 (c) of this Agreement shall survive the termination of this Agreement.

(g) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with the applicable requirements under HIPAA and other applicable law or regulation.

IN WITNESS WHEREOF, the parties have signed this Agreement on the date indicated below.

**NAME OF BUSINESS ASSOCIATE**

**SOUTH CAROLINA PUBLIC EMPLOYEE  
BENEFIT AUTHORITY**

By: \_\_\_\_\_

By: \_\_\_\_\_

(Signature)

(Signature)

NAME: \_\_\_\_\_

NAME: \_\_\_\_\_

(Type or Print Name)

(Type or Print Name)

TITLE: \_\_\_\_\_

TITLE: \_\_\_\_\_

DATE: \_\_\_\_\_

DATE: \_\_\_\_\_



**Attachment One (1)**  
**Non-Disclosure Agreement**

This Non-Disclosure Agreement (the "Agreement") is made this \_\_\_\_ day of \_\_\_\_\_ 201\_, by and between \_\_\_\_\_ (hereinafter referred to as "the Offeror ") and the State of South Carolina, South Carolina Public Employee Benefit Authority (hereinafter referred to as "the State"). Offeror as herein used includes both any entity that submits a proposal and any entity that is considering submitting a proposal but ultimately does not.

Offeror warrants and represents that it intends to submit a Services/Technical Proposal in response to the Request for Proposals for Pharmacy Benefit Management Services for the State Health Plan. In order for the Offeror to submit a Proposal, it will be necessary for the State to provide the Offeror with access to certain confidential information including, but not limited to, demographic and identifying information on eligible individuals and plan utilization data. All such information provided by the State shall be considered Confidential Information regardless of the form, format, or media upon which or in which such information is contained or provided, regardless of whether it is oral, written, electronic, or any other form, and regardless of whether the information is marked as "Confidential Information." As a condition for its receipt and access to the Confidential Information described in Part II, Scope of Proposal, Introduction, Offeror agrees as follows:

1. Offeror will not copy, disclose, publish, release, transfer, disseminate or use for any purpose in any form any Confidential Information received except in connection with the preparation of its Proposal. All Confidential Information and copies thereof shall be protected from disclosure by commercially reasonable means, including without limitation physical separation, security and limited need to know access for any hard copy materials and encryption, password protection, and secure transmission for electronic materials respectively.
2. Each employee or agent (including without limitation subcontractors) of the Offeror who receives or has access to the Confidential Information shall be notified of the confidentiality and nondisclosure requirements of this Agreement and the confidential nature of the Confidential Information. Each employee or agent of the Offeror who is provided access to or a copy of the Confidential Information shall be bound by confidentiality and nondisclosure obligations that are no less restrictive than the obligations set forth herein. The Offeror shall be liable for any violations by any employees or agents who are provided or given access to Confidential Information. The Offeror shall provide a list of all individuals, employees, and agents of the Offeror who have or have had access to the Confidential Information, along with the certification required in Section 3 of this Agreement.
3. Offeror, other than the Contractor, shall return to the State the original and destroy (in a manner designed to prohibit reading of, copying or reconstruction of the data) any copies of the Confidential Information remaining in its possession within five (5) business days of the State's notice of award in connection with this procurement. If any Offeror does not submit a Proposal, the Offeror shall return the Confidential Information to the Procurement Officer on or before the due date for Proposals. The Offeror, other than the Contractor, shall certify, in writing and signed by an individual with authority to bind the Offeror, to the Procurement Officer that any and all Confidential Information (in whatever format or media) has been destroyed or returned to the Procurement Officer within five (5) business days of the notice of award or by the date the Offeror will not or did not submit a proposal, whichever is earlier. Such certification may be in the form provided below or in another form.
4. Offeror acknowledges that the disclosure of the Confidential Information may cause irreparable harm to the State and agrees that the State may obtain an injunction to prevent the disclosure, copying, or other impermissible use of the Confidential Information. The State's rights and remedies hereunder are cumulative and the State expressly reserves any and all rights, remedies, claims and actions that it may have now or in the future to protect the Confidential Information and/or to seek damages for the Offeror's failure

to comply with the requirements of this Agreement. The Offeror consents to personal jurisdiction in the South Carolina State Courts.

5. In the event the State suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part to any failure by the Offeror or any employee or agent of the Offeror to comply with the requirements of this Agreement, Offeror shall hold harmless and indemnify the State from and against any such losses, damages, liabilities, expenses, and/or costs.
6. This Agreement shall be governed by the laws of the State of South Carolina.
7. Offeror acknowledges that a person may not willfully make a false or fraudulent statement or representation of a material fact in connection with a procurement contract. Offeror further acknowledges that this Agreement is a statement made in connection with a procurement contract.
8. The individual signing below warrants and represents that he or she is fully authorized to bind the Offeror to the terms and conditions specified in this Agreement.

OFFEROR: \_\_\_\_\_

BY: \_\_\_\_\_  
Signature

NAME: \_\_\_\_\_  
Print Name

TITLE: \_\_\_\_\_

ADDRESS: \_\_\_\_\_

OFFEROR'S EMPLOYEES AND AGENTS WHO WILL BE GIVEN ACCESS TO THE CONFIDENTIAL INFORMATION

Printed Name and Address of Individual/Agent	Employee (E) or Agent (A)
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____





**Attachment Two (2)**  
**Business Associate Contract**

THIS AGREEMENT is entered into as of the \_\_\_ day of \_\_\_\_\_, \_\_\_\_\_ between **NAME, ADDRESS** (hereinafter referred to as “Business Associate”) and the South Carolina Public Employee Benefit Authority, 202 Arbor Lake Drive, Columbia, South Carolina 29223 (hereinafter referred to as the “Covered Entity”).

WHEREAS, the Privacy Rule (as defined below) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) permits group health plans to disclose certain Protected Health Information of a patient to a Business Associate of such plan who performs certain functions or activities on behalf of the plan, provided that the plan enters into an agreement with the Business Associate that limits the use and disclosure of such Protected Health Information to the same extent that such limitations apply to the group health plan;

WHEREAS, the Security Rule (as defined below) established national standards to protect individuals’ electronic personal health information; and

WHEREAS, the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), pursuant to Title XIII of Division A and Title IV of Division B, called the “Health Information Technology for Economic and Clinical Health” (“HITECH Act”), provides modifications to the HIPAA Security and Privacy Rule (hereinafter, all references to the “HIPAA Security and Privacy Rule” are deemed to include all amendments to such rule contained in the HITECH Act and any accompanying regulations, and any other subsequently adopted amendments or regulations); and

WHEREAS, Covered Entity is a self-funded group health plan, and Business Associate provides such functions or activities on behalf of the Covered Entity as to constitute a “Business Associate” of the Covered Entity, as defined in the Privacy Rule;

WHEREAS, Covered Entity and Business Associate have heretofore entered into a separate Service Agreement;

WHEREAS, Covered Entity and Business Associate do hereby desire to enter into this Agreement as required under the Security and Privacy Rule and the provisions of the HITECH Act;

NOW, THEREFORE, for the reasons set forth above, and in consideration of the mutual promises and agreements set forth herein, Covered Entity and Business Associate do hereby contract and agree as follows:

**1. DEFINITIONS**

- (p) “Business Associate” shall mean **NAME**.
- (q) “Compliance Date” shall have the same meaning as the term “Compliance Date” in 45 CFR § 160.103.
- (r) “Covered Entity” shall mean the South Carolina Public Employee Benefit Authority.
- (s) “Data Aggregation” shall have the same meaning as the term “Data Aggregation” in 45 CFR § 164.501.
- (t) “Designated Record Set” shall have the same meaning as the term “Designated Record Set” in 45 CFR § 164.501.
- (u) “Electronic Protected Health Information” shall have the same meaning as “Electronic Protected Health

Information” in 45 CFR §160.103. “HITECH Act” shall have the same meaning as the Health Information Technology for Economic and Clinical Health Act, as incorporated into the American Recovery and Reinvestment Act of 2009.

- (v) “Individual” shall have the same meaning as the term “Individual” in 45 CFR §164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
- (w) “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and 164, subparts A and E.
- (x) “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” in 45 CFR § 160.103, limited to the information created or received by Business Associate from, or on behalf of, Covered Entity.
- (y) “Required By Law” shall have the same meaning as the term “Required By Law” in 45 CFR § 164.103.
- (z) “Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her designee.
- (aa) “Security Incident” shall have the same meaning as “Security Incident” in 45 CFR § 164.304.
- (bb) “Security Rule” shall mean the Security Standards and Implementation Specifications at 45 CFR Part 160 and 164, Subpart C.
- (cc) “Service Agreement” shall mean the agreement between **NAME** and the South Carolina Public Employee Benefit Authority, whereby **NAME** performs plan management and plan administrative tasks on behalf of the benefit program described herein as Covered Entity.
- (dd) “Standards for Electronic Transactions Rule” means the final regulations issued by the Department of Health and Human Services concerning standard transactions and code sets under the Administration Simplification provisions of HIPAA, 45 CFR Part 160 and Part 162.

## **2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE**

- (v) Business Associate agrees to use or disclose PHI only as permitted or required by this Agreement or as Required By Law. Business Associate is permitted to use and disclose PHI or Electronic PHI that it creates for, or receives from, Covered Entity or business associate of Covered Entity and to request PHI on behalf of Covered Entity as described in the Agreement, consistent with the HIPAA Privacy and Security Rules. When requesting, using, or disclosing PHI, Business Associate shall restrict the request, use, or disclosure of said PHI to the minimum necessary to accomplish the intended purpose of the request, use, or disclosure **in accordance with, and subject to the exceptions in, 45 CFR 164.502(b).**
- (w) Business Associate agrees to provide access to Covered Entity, at the request of Covered Entity, to PHI in a Designated Record Set in order to meet the requirements under 45 CFR § 164.524.
- (x) Business Associate agrees to make available PHI for amendment and incorporate any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity, within thirty (30) days of a written request by Covered Entity.

(y) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by, Business Associate on behalf of Covered Entity available to the Covered Entity or the Secretary, within thirty (30) days of a written request by the Covered Entity or the Secretary, for the purpose of permitting the Secretary to determine Covered Entity's compliance with the HIPAA Privacy and Security Rules.

(z) Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528 and to make available to Covered Entity, within thirty (30) days of a written request by Covered Entity, the information required to provide such an accounting to an individual. Business Associate will comply with mandates regarding individuals' rights under the HITECH Act, including rights to access and accounting of disclosures. Such information shall be made available in an electronic format where directed by Covered Entity. In addition, Business Associate shall include, within its accounting, disclosures for payment and health care operations purposes where such recording or accounting is required by the HITECH Act and as of the effective date for this provision of the HITECH Act. Covered Entity shall provide any additional information to the extent required by the HITECH Act and any accompanying regulations.

(aa) Business Associate shall make information available directly to an individual within thirty (30) days, when that individual so requests, if such information is required to be disclosed under the HITECH Act and/or accompanying regulations.

(bb) Business Associate agrees to develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Covered Entity's electronic and paper PHI that Business Associate creates, receives, maintains, or transmits on Covered Entity's behalf, as required by the HIPAA Security Rule and as required by the HITECH Act. Business Associate shall also develop and implement policies and procedures and meet the HIPAA Security Rule documentation requirements as required by the HITECH Act.

(cc) Business Associate agrees to ensure that any agent, including a subcontractor, to whom Business Associate provides PHI, agrees to abide by the same restrictions and conditions that apply to Business Associate with respect to PHI in conformance with the Privacy Rule, and to implement reasonable and appropriate safeguards to protect it.

(dd) Business Associate agrees to notify Covered Entity within two (2) business days of becoming aware of any use or disclosure of PHI not provided for by the Agreement, and within **twenty-four (24) hours** minutes of any security incident resulting in the successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system, or resulting in any "Breach" of "Unsecured Protected Health Information," as these terms are defined by the HITECH Act and any implementing regulations.

(ee) Business Associate agrees to mitigate, to the extent practicable, any harmful effect it knows to have resulted from said Breach. Any such report shall include, to the extent possible, the identification (if known) of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Breach, along with any other information required to be reported under the HITECH Act and any accompanying regulations.

(ff) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

(gg) Business Associate agrees to maintain appropriate clearance procedures and provide supervision to ensure that its workforce follows Business Associate's security procedures.

(hh) Business Associate agrees to provide appropriate training for its staff to ensure that its staff complies with its privacy and security policies.

(ii) Business Associate agrees to implement appropriate security incident procedures and provide training to its applicable staff sufficient to detect and analyze security incidents.

(jj) Business Associate agrees to maintain a current contingency plan in case of an emergency.

(kk) Business Associate agrees, as appropriate, to maintain an emergency access plan to ensure that the PHI it holds on behalf of Covered Entity is available when needed.

(ll) Business Associate agrees to implement appropriate storage, disposal and reuse procedures to protect any PHI that Business Associate holds for Covered Entity.

(mm) Business Associate agrees to provide appropriate backup of the PHI that Business Associate holds for Covered Entity.

(nn) Business Associate agrees to have in place appropriate authentication and access controls to safeguard the PHI that Business Associate holds for Covered Entity.

(oo) Business Associate agrees to make use of encryption, as appropriate, when transmitting PHI over the Internet.

(pp) Business Associate agrees to retain the documentation required by this agreement for six years from the date of its creation or the date when it last was in effect, whichever is later.

Covered Entity and Business Associate recognize and agree that in some instances **NAME** may have compliance obligations as a Health Care Provider under the Privacy Rule and nothing herein shall prohibit, restrict, or otherwise limit compliance with any such obligations by **NAME** under the Privacy Rule.

## **8. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION BY BUSINESS ASSOCIATE**

(f) Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities or services for, or on behalf of, Covered Entity, as specified in the Service Agreement, provided that such use or disclosure would not violate the Privacy and Security Rules if done by Covered Entity.

(g) Except as otherwise limited in this agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(h) Except as otherwise limited in this agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate if the disclosures are Required By Law; or if Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the PHI will remain confidential and will be used or further disclosed only as Required By Law or only for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(i) Except as otherwise limited in this agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

(j) Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).

(f) Business Associate may also use and disclose PHI: (i) to respond to requests for PHI either accompanied by an authorization that meets the requirements of 45 CFR 164.508 or from a covered entity or health care provider in accordance with 45 CFR 164.506(c); (ii) to de-identify the information or create a limited data set in accordance with 45 CFR §164.514, which de-identified information or limited data set may be used and disclosed by Business Associate as permitted by law, including HIPAA; and (iii) as authorized in writing by Covered Entity

## 9. OBLIGATIONS OF COVERED ENTITY

(d) Covered Entity shall notify Business Associate of any limitations in its notice(s) of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitations may affect Business Associate's use or disclosure of PHI.

(e) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(f) Covered Entity shall notify Business Associate 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 Business Associate's use or disclosure of PHI.

## 10. PERMISSIBLE REQUESTS BY COVERED ENTITY

Covered Entity shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under the Security and Privacy Rules if done by Covered Entity, except Business Associate may use or disclose PHI for data aggregation or management and administrative activities of Business Associate.

## 11. TERM AND TERMINATION

(d) Ter  
m.

The Term of this Agreement and the obligations herein shall be deemed effective as of the Compliance Date or the date of execution of this Agreement, whichever date is later, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or if it is not feasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

(e) Termination for Cause.

Upon either Party's (the Non-Breaching Party's) knowledge of a material breach by the other party (the Breaching Party), the Non-Breaching Party may:

(3) Provide an opportunity for the Breaching Party to cure the material breach or end the violation and terminate this Agreement if the Breaching Party does not cure the material breach or end the violation within the reasonable time specified by the Non-Breaching Party; or

(4) If neither termination nor cure is feasible, the Non-Breaching Party may report the violation to the Secretary. Failure by the Non-Breaching Party to exercise its rights to terminate under this provision shall not be construed as a waiver of its rights to terminate, rescind or revoke the services herein in case of any subsequent breach.

(f) Effect \_\_\_\_\_ of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

(2) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible, including the need to retain PHI for audit, justification of work product or compliance with other applicable law. Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI

## 12. MISCELLANEOUS

(h) Definitions. All terms that are used but not otherwise defined in this Supplement shall have the meaning specified under HIPAA, including its statute, regulations, and other official government guidance.

(i) Independent Contractor. The relationship between the parties will solely be that of independent contractors engaged in the operation of their own respective businesses.

(j) Third Party Beneficiaries. The parties agree that there are no intended third party beneficiaries under this Agreement.

(k) Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect, or as amended, and for which compliance is required.

(l) Amendment. The parties agree to take such action as is necessary to amend this Agreement as is necessary to comply with the requirements of HIPAA and other applicable law or regulation.

(m) Survival. The respective rights and obligations of Business Associate under Section 6 (c) of this Agreement shall survive the termination of this Agreement.

(n) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with the applicable requirements under HIPAA and other applicable law or regulation.

IN WITNESS WHEREOF, the parties have signed this Agreement on the date indicated below.

**NAME OF BUSINESS ASSOCIATE**

**SOUTH CAROLINA PUBLIC EMPLOYEE  
BENEFIT AUTHORITY**

By: \_\_\_\_\_

By: \_\_\_\_\_

(Signature)

(Signature)

NAME: \_\_\_\_\_

NAME: \_\_\_\_\_

(Type or Print Name)

(Type or Print Name)

TITLE: \_\_\_\_\_

TITLE: \_\_\_\_\_

DATE: \_\_\_\_\_

DATE: \_\_\_\_\_

**Attachment Three (3)**  
**Service Provider Security Assessment Questionnaire**

**SERVICE PROVIDER SECURITY ASSESMENT QUESTIONNAIRE**

**Instructions: I. Attach additional pages or documents as appropriate.**

**II. As used in this Questionnaire, government information shall have the meaning defined in the clause titled “Information Security.”**

1. Describe your policies and procedures that ensure access to government information is limited to only those employees/Contractors who require access to perform your proposed services.
2. Describe your disaster recovery and business continuity plans.
3. What safeguards and practices do you have in place to vet employees and Contractors who have access to government information?
4. Describe and explain your security policies and procedures related to use of Contractors/sub -contractors.
5. List any certifications that you have that demonstrate that adequate security controls are in place to properly store, manage and process government information (for example, ISO or SSAE certifications). Will these certifications be in place for the duration of the contract? Will you provide the state with most recent and future audit reports related to these certifications?
6. Describe the policies, procedures and practices you have in place to provide for the physical security of your data centers and other sites where government information will be hosted, accessed or maintained.
7. Will government information be encrypted at rest? Will government information be encrypted when transmitted? Will government information be encrypted during data backups?
8. Describe safeguards that are in place to prevent unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access or disclosure of government information.
9. What controls are in place to detect security breaches? Do you log transactions and network activity? How long do you maintain these audit logs?
10. How will government information be managed after contract termination? Will government information provided to the Contractor be deleted or destroyed? When will this occur?
11. Describe your incident response policies and practices.
12. Identify any third party which will host or have access to government information.

**Offeror’s response to this questionnaire includes any other information submitted with its offer regarding information or data security.**

**SIGNATURE OF PERSON AUTHORIZED TO REPRESENT THE ACCURACY OF THIS INFORMATION ON BEHALF OF CONTRACTOR:**

By: \_\_\_\_\_  
(Authorized Signature)

Its: \_\_\_\_\_  
(Printed name of person signing above)

Date: \_\_\_\_\_  
(Title of person signing above)



**Attachment Four (4)  
Co-Pay Waiver Drugs**

**The following three items comprise Attachment 4. The attachment is posted separately.**

**Antihypertensive Drug List  
Cholesterol-Lowering Drug List  
Diabetes Drugs and Testing Supplies**

**Attachment Five (5)**  
**Clinical Benefit Template**

**The attachment is posted separately.**

**Attachment Six (6)**  
**Participating Pharmacies**

**The attachment is posted separately.**

**Attachment Seven (7)**  
**EGWP Formulary**

**The attachment is posted separately.**

**Attachment Eight (8)**  
**Comprehensive Formulary**

**The attachment is posted separately.**

**Attachment Nine (9)**  
**PEBA Utilization Management List**

**The attachment is posted separately**

**Attachment Ten (10)**  
**Questions and Answers**

**The attachment is posted separately.**