ATTACHMENT 2

SAMPLE BUSINESS ASSOCIATE AGREEMENT

AGREEMENT WITH BUSINESS ASSOCIATE

This ("Agreement") is effective upon full execution, by and between **{Insert Operating Company Name}** _____ ("Business Associate") and **{Insert Group Health Plan Name}** _____ ("Group Health Plan").

Group Health Plan and Business Associate mutually agree to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160-164) and any applicable state privacy laws.

Privacy of Protected Health Information and Nonpublic Personal Financial Information.

1. **Permitted Uses and Disclosures.** Business Associate (and any subcontractor or agent) is permitted or required to use or disclose Protected Health Information ("PHI") it creates for or receives from Group Health Plan only as follows:

   a) Functions and Activities on Group Health Plan's Behalf. Business Associate is permitted to use and disclose the minimum necessary PHI created for or received from Group Health Plan solely as necessary to perform its obligations to Group Health Plan as set forth in the Agreement.

   b) Business Associate's Operations. Business Associate may use the minimum necessary PHI created for or received from Group Health Plan solely as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities under the Agreement. Business Associate may disclose such minimum necessary PHI only as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities under the Agreement only if:

      (i) The disclosure is required by law; or

      (ii) Business Associate obtains reasonable assurance, evidenced by written contract, from any person or organization to which Business Associate will disclose such PHI that the person or organization will***:***

      (aa) Hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization or as required by law; and

      (bb) Notify Business Associate (who will in turn promptly notify Group Health Plan) of any instance of which the person or organization becomes aware of any non-permitted use or disclosure or [BJF Addition.] in which the confidentiality of such PHI was breached.

2. **Prohibition on Unauthorized Use or Disclosure.** Business Associate will neither use nor disclose PHI it creates for or receives from Group Health Plan or from another Business Associate of Group Health Plan, except as permitted or required by this Addendum or as required by law or as otherwise permitted in writing by Group Health Plan.

3. **Information Safeguards.** Business Associate will use reasonable and appropriate [BJF addition] administrative, technical and physical safeguards, in compliance with Social Security Act § 1173(d) (42 U.S.C. § 1320d-2(d)), 45 C.F.R. § 164.530(c) and any other applicable implementing regulations issued by the U.S. Department of Health and Human Services to preserve the integrity, confidentiality and availability of and to prevent unauthorized or prohibited use or disclosure of PHI created for or received from Group Health Plan.

4. **Sub-Contractors and Agents.** Business Associate will require its subcontractors and agents, to which Business Associate is permitted by this Addendum or in writing by Group Health Plan to disclose any of the PHI Business Associate creates for or receives from Group Health Plan, to provide reasonable assurance, evidenced by a written contract, that subcontractor or agent will

comply with the same privacy, security, and other obligations as Business Associate with respect to such PHI.

5. **Compliance with Standard Transactions.** If Business Associate conducts Standard Transactions (45 C.F.R. Parts 160 and 162) with or on behalf of Group Health Plan, Business Associate will comply will require any subcontractor or agent involved with the conduct of such Standard Transactions to comply, with each applicable requirement of 45 C.F.R. Part 162. Business Associate agrees to demonstrate compliance with the Transactions by allowing Group Health Plan to test the Transactions and content requirements upon a mutually agreeable date. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of Group Health Plan that:

   a) Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;

   b) Adds any data elements or segments to the maximum defined data set;

   c) Uses any code or data element that is marked "not used" in the Standard Transaction's implementation specification or is not in the Standard Transaction's implementation specification; or

   d) Changes the meaning or intent of the Standard Transaction's implementation specification.

6. **Security of Electronic Protected Health Information**: If Business Associate receives or maintains Electronic Protected Health Information, Business Associate will comply (and will require any subcontractor or agent that receives or maintains such Electronic Protected Health Information to comply) with the following in addition to all other provisions of this Addendum:

   a) Business Associate shall require its agents and subcontractors to provide data security for all Electronic Protected Health Information.

   b) Business Associate shall implement and maintain, and shall require its agents and subcontractors to implement and maintain, reasonable administrative, technical and physical safeguards to protect the security, integrity and confidentiality of Electronic Protected Health Information.

7. **Protected Health Information Access, Amendment and Disclosure Accounting.**

   a) **Access.** Business Associate (and any subcontractor or agent) will promptly, upon Group Health Plan's request, make available to Group Health Plan or, at Group Health Plan's direction, to the individual (or the individual's personal representative) for inspection and obtaining copies of any PHI about the individual which Business Associate created for or received from Group Health Plan and that is in Business Associate's custody or control, so that Group Health Plan may meet its access obligations under 45 C.F.R. § 164.524.

   b) **Amendment.** Business Associate will accept requests for access to or copies of PHI forwarded from Group Health Plan or received from an individual (or the individual's personal representative) directly. Business Associate (and any subcontractor or agent) will, upon receipt of notice from Group Health Plan, promptly amend or permit Group Health Plan access to amend any portion of the PHI which Business Associate created for or received from Group Health Plan, so that Group Health Plan may meet its amendment obligations under 45 C.F.R. § 164.526.

   c) **Disclosure Accounting.** So that Group Health Plan may meet its disclosure accounting obligations under 45 C.F.R. § 164.528:

      (i) Disclosure Tracking. Business Associate (and any subcontractor or agent) will record for each disclosure of PHI that Business Associate creates for or receives from Group Health Plan that is not excepted from disclosure accounting under Addendum section 7.c)(ii) below ("Exceptions from Disclosure Tracking"), that Business Associate makes to Group Health Plan or a third party: (i) the disclosure date, (ii) the name and (if known) address of the person or entity to whom Business Associate made the disclosure, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of the disclosure (items i-iv,

collectively, the "disclosure information"). For repetitive disclosures Business Associate makes to the same person or entity (including Group Health Plan) for a single purpose, Business Associate may provide (x) the disclosure information for the first of these repetitive disclosures, (y) the frequency, periodicity or number of these repetitive disclosures and (z) the date of the last of these repetitive disclosures. Business Associate will make this disclosure information available to Group Health Plan promptly upon Group Health Plan's request, but in no event later than fourteen (14) days following receipt of the request.

(ii) Exceptions from Disclosure Tracking. Business Associate (and any subcontractor or agent) need not record disclosure information or otherwise account for disclosures of PHI that this Addendum or Group Health Plan in writing permits or requires (i) for the purpose of treatment activities, payment activities, or health care operations; (ii) to the individual who is the subject of the PHI disclosed or to that individual's personal representative; (iii) to persons involved in that individual's health care or payment for health care; (iv) for notification for disaster relief purposes, (v) for national security or intelligence purposes; or (vi) to law enforcement officials or correctional institutions regarding inmates.

(iii) Disclosure Tracking Time Periods. Business Associate (and any subcontractor or agent) must have available for Group Health Plan the disclosure information required by Addendum section 7.c)(i) ("Disclosure Tracking") for the six (6) years preceding Group Health Plan's request for the disclosure information (except Business Associate need not have disclosure information for disclosures occurring before April 14, 2003).

d) Restriction Agreements and Confidential Communications. Business Associate (and any subcontractor or agent) will comply with any agreement that Group Health Plan makes that either (i) restricts use or disclosure of Group Health Plan's PHI pursuant to 45 C.F.R. § 164.522(a), or (ii) requires confidential communication about Group Health Plan's PHI pursuant to 45 C.F.R. § 164.522(b), provided that Group Health Plan notifies Business Associate in writing of the restriction or confidential communication obligations that Business Associate must follow. Group Health Plan agrees to consult with Business Associate before agreeing to any requests for restriction or confidential communication from individuals, to ensure that Business Associate is able to accommodate any such requests. Group Health Plan will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of Group Health Plan's PHI will remain subject to the terms of the restriction agreement.

e) Inspection of Books and Records. Business Associate (and any subcontractor or agent) will make its internal practices, books, and records, relating to its use and disclosure of the PHI it creates or receives for or from Group Health Plan, available to the U.S. Department of Health and Human Services to determine Group Health Plan's compliance with 45 C.F.R. Parts 160 and 164.

8. Breach of Privacy Obligations.

a) **Reporting.** Business Associate will promptly report to Group Health Plan in writing any use or disclosure of PHI not permitted by this Addendum or by Group Health Plan. Business Associate will promptly provide Group Health Plan with information regarding the nature and extent of the improper use or disclosure and any additional information the Group Health Plan may reasonably request.

b) **Correction and Mitigation.** Business Associate agrees to make all reasonable efforts to correct and mitigate, to the extent practicable or as directed by Group Health Plan, and at Business Associate's own expense, any harmful effect, under its control, that is known to Business Associate resulting from its breach of this Addendum or the Agreement.

c) **Security Incidents.** If a security incident results in a disclosure of Group Health Plan's Electronic Protected Health Information (EPHI) not permitted by this Addendum, Business Associate will promptly report such incident to Group Health Plan. Business Associate will report to Group Health Plan any unauthorized:

(i) access, use, disclosure, modification or destruction of Group Health Plan's EPHI of which Business Associate becomes aware; or

(ii) interference with system operations in Business Associate's information systems involving Group Health Plan's EPHI of which Business Associate becomes aware.

d) Termination of Agreement.

(i) Material Breach. Business Associate agrees that Group Health Plan has the right to terminate the Agreement if Group Health Plan determines that Business Associate or Agent or Subcontractor of Business Associate has violated a material term of this Addendum and such violation continues for ten (10) days after written notice of such violation has been given to Business Associate by Group Health Plan. [45 CFR § 164.504(e)]

(ii) Obligations upon Termination.

(aa) Return or Destruction. Upon termination, cancellation, expiration or other conclusion of the Agreement, Business Associate will, if feasible, return to Group Health Plan or destroy all PHI, in whatever form or medium (including in any electronic medium under Business Associate's custody or control), that Business Associate (or its subcontractors or agents) created for or received from Group Health Plan, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI. Business Associate will complete such return or destruction as promptly as possible, but not later than 60 days after the effective date of the termination, cancellation, expiration or other conclusion of the Agreement. Business Associate will identify any PHI that Business Associate (or its subcontractors or agents) created for or received from Group Health Plan that cannot feasibly be returned to Group Health Plan or destroyed, and will limit its further use or disclosure of that PHI to those purposes that make return or destruction of that PHI infeasible. Within such 60 days, Business Associate will certify on oath in writing to Group Health Plan that such return or destruction has been completed, will deliver to Group Health Plan the identification of any PHI for which return or destruction is infeasible and, for that PHI, will certify that it will only use or disclose such PHI for those purposes that make return or destruction infeasible.

(bb) Continuing Privacy Obligation. Business Associate's obligation (and the obligation of Business Associate's subcontractors or agents) to protect the privacy of the PHI it created for or received from Group Health Plan will be continuous and survive termination, cancellation, expiration or other conclusion of the Agreement.

(cc) Other Obligations and Rights. Business Associate's other obligations and rights and Group Health Plan's obligations and rights upon termination, cancellation, expiration or other conclusion of the Agreement will be those set out in the termination provisions of the Agreement.

9. **General Provisions**.

a) Definitions.

Individually Identifiable Health Information ("IIHI") is information that is a subset of health information, including demographic information collected from an individual, and:

(i) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(ii) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past present or future payment for the provision of health care to an individual; and

(aa) That identifies the individual; or

(bb) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

***Protected Health Information* (“*PHI*”)** means individually identifiable health information created, received, used, or disclosed in connection with the Agreement:

(i) that is:

(aa) Transmitted by electronic media;

(bb) Maintained in any medium described in the definition of *electronic media* at § 160.103; or

(cc) Transmitted or maintained in any other form or medium.

Electronic Protected Health Information means the subset of information created, received, used, or disclosed in connection with the Agreement described in subparagraphs (aa) and (bb) of the definition of ***Protected Health Information,*** as specified in this section above. For purposes of this Addendum, when reference is made to *“Electronic Protected Health Information”* or *“EPHI”* (rather than *“Protected Health Information”* or *“PHI”)*, the obligations of this Addendum shall apply only to *EPHI*, and not the broader category of *PHI*.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information **within** an entity that maintains or has possession of such information.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information **outside** the entity holding the information.

b) **Amendment to Agreement.** The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of the Agreement may be required to ensure compliance with changes in the laws or regulations. The parties specifically agree to take such action necessary to implement the standards and requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the implementing regulations issued by the U.S. Department of Health and Human Services (45 C.F.R. Parts 160-164). Upon Group Health Plan’s reasonable request, Business Associate agrees to promptly amend the terms of this Addendum to conform to any applicable change in law or regulation, subject to any rights Business Associate has under the Agreement to adjust its fees thereunder. Business Associate agrees to promptly amend its agreements with its subcontractors and agents to conform to the terms of the Addendum. Group Health Plan may terminate the Agreement upon forty-five (45) days written notice in the event (i) Business Associate does not promptly amend the Addendum to the Agreement when requested by Group Health Plan pursuant to this Section, or (ii) Business Associate does not amend the Addendum sufficient to satisfy the standards and requirements the HIPAA regulations.

Conflicts. The terms and conditions of this Addendum will override and control any conflicting terms or condition of the Agreement. All non-conflicting terms and conditions of the Agreement remain in full force and effect.

IN WITNESS WHEREOF, Group Health Plan and Business Associate execute this Addendum in multiple originals to be effective upon full execution, as indicated by the last date written below.

{Insert Business Associate’s Name }	**{Insert Group Health Plan’s name}**
By: _____	By: _____
Its: _____	Its: _____
Date: _____	Date: _____