BUSINESS ASSOCIATE AGREEMENT

This agreement ("Agreement") is effective on the date executed by Business Associate and is between the Brokerage/Broker/Agency/Agent named in the execution process of this Agreement ("Business Associate") and Golden West Health Plan, Inc. and its affiliated companies who are Covered Entities or Business Associates and who have a business relationship with Business Associate, if any (hereinafter collectively "Company"). The purpose of this Agreement is to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 C.F.R. Parts 160-64), any applicable state privacy laws, any applicable state security laws, any applicable implementing regulations issued by the Insurance Commissioner or other regulatory authority having jurisdiction and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act") and any regulations adopted or to be adopted pursuant to the HITECH Act that relate to the obligations of business associates. Business Associate recognizes and agrees it is obligated by law to meet the applicable provisions of the HITECH Act.

All capitalized terms in this Agreement that are not defined in this Agreement will have the meaning ascribed to those terms by 45 C.F.R. Parts 160-164, or applicable insurance regulations that are applicable to Company's relationship with Business Associate.

A. Privacy of Protected Health Information and Nonpublic Personal Financial Information.

1. **Permitted and Required Uses and Disclosures.** Business Associate is permitted or required to Use or disclose Protected Health Information ("PHI") it requests, creates or receives for or from Company (or another business associate of Company) only as follows:

   a) Functions and Activities on Company's Behalf. Business Associate is permitted to request, Use and disclose PHI it creates or receives for or from Company (or another business associate of Company), consistent with the Privacy Rule and the HITECH Act, only as described in this Agreement, or other agreements during their term that may exist between Company and Business Associate.

   b) Business Associate's Operations. Business Associate may Use PHI it creates or receives for or from Company as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities. Business Associate may disclose such PHI as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities 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:

         a. 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

         b. Notify Business Associate (who will in turn promptly notify Company) of any instance of which the person or organization becomes aware in which the confidentiality of such PHI was breached.

   c) Data Aggregation Services. If specifically directed by the Company, the Business Associate will provide Data Aggregation services relating to the Health Care Operations of the Company.

d) Minimum Necessary and Limited Data Set. In any instance when Business Associate Uses, requests or discloses PHI under this Agreement or in accordance with other agreements that exist between Company and Business Associate, Business Associate shall utilize a Limited Data Set, if practicable. Otherwise, Business Associate may Use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose, except that Business Associate will not be obligated to comply with this minimum necessary limitation with respect to:

(i) Disclosure to or request by a Health Care Provider for Treatment;
(ii) Use for or Disclosure to an Individual who is the subject of Company's PHI, or that Individual's Personal Representative;
(iii) Use or Disclosure made pursuant to an authorization compliant with 45 C.F.R. §164.508 that is signed by an Individual who is the subject of Company's PHI to be used or disclosed, or by that Individual's Personal Representative;
(iv) Disclosure to the United States Department of Health and Human Services ("HHS") in accordance with Section C(5) of this Agreement;
(v) Use or Disclosure that is Required by Law; or
(vi) Any other Use or Disclosure that is excepted from the Minimum Necessary limitation as specified in 45 C.F.R. §164.502(b)(2).

e) Use by Workforce. Business Associate shall advise members of its workforce of their obligations to protect and safeguard PHI. Business Associate shall take appropriate disciplinary action against any member of its workforce who uses or discloses PHI in contravention of this Agreement.

2. **Prohibitions on Unauthorized Requests, Use or Disclosure.**

a) Business Associate will neither Use nor disclose Company's PHI it creates or receives from Company or from another Business Associate of Company, except as permitted or required by this Agreement or as Required by Law or as otherwise permitted in writing by Company. This Agreement does not authorize Business Associate to request, Use, disclose, maintain or transmit PHI in a manner that will violate 45 C.F.R. Parts 160-164.

b) Business Associate will not develop any list, description or other grouping of Individuals using PHI received from or on behalf of Company, except as permitted by this Agreement or in writing by Company. Business Associate will not request, Use or disclose any list, description or other grouping of Individuals that is derived using such PHI, except as permitted by this Agreement or in writing by Company.

3. **Sub-Contractors and Agents.** Business Associate will require any of its subcontractors and agents to provide reasonable assurance, evidenced by written contract, that subcontractor or agent will comply with the same privacy and security obligations as Business Associate with respect to such PHI, including the obligations described in Section 4 herein.

4. Information Safeguards. Business Associate must implement, maintain and use a written information security program that contains the necessary administrative, technical and physical safeguards that are appropriate in light of the Business Associate's size and complexity in order to achieve the safeguarding objectives as detailed in Social Security Act § 1173(d) (42 U.S.C. § 1320d-2(d)), 45 C.F.R. Part 164.530(c), the HITECH Act and any other implementing regulations issued by the U.S. Department of Health and Human Services, as such may be amended from time to time and as required by the WellPoint Information Security Program. Business Associate shall notify Company should Business Associate determine it is unable to comply with any such law, regulation or official guidance. Further, Business Associate shall comply with any applicable state data security law. In furtherance of compliance with such requirements, Business Associate shall:

1. Maintain a privacy policy and procedure for Business Associate's organization, which must identify an officer of the organization that is responsible for enforcement.
2. All employees of Business Associate that handle or access PHI must undergo ongoing training regarding the safeguarding of PHI.
3. Ensure that any third party that Business Associate contracts with or relies upon for the provision of services to WellPoint also maintains a framework for compliance with the HIPAA Privacy and Security rules.
4. Implement a contingency plan for responding to emergencies and/or disruptions in your business, to ensure, to the extent reasonable, that services provided to WellPoint are not interrupted and the integrity and safety of all PHI is maintained.
5. Establish and implement a data back up program that ensures Business Associates' ability to provide Company with retrievable, exact copies of PHI, upon Company's request.
6. Maintain and exercise an audit plan to respond to internal and external security threats and violations. The audit plan should document the scope and frequency of audits and the audit procedure.
7. Document how security breaches that are discovered will be addressed.
8. Maintain technology policies and procedures that ensure the protection of PHI on hardware and software utilized by Business Associate.
9. Maintain all PHI received or created in paper form in a secure location with restricted access.
10. Utilize encryption for the electronic transmission of PHI to Company and/or to any other third party, as directed by Company or as required for the provision of services to Company.
11. To the extent that Business Associate stores, processes and/or transmits cardholder data (e.g., credit card numbers and other related information, as such term is defined by the Payment Card Industry, (PCI) Data Security Standards), Business Associate shall comply with all PCI Data Security Standards.

Business Associate shall provide Company with information concerning the aforementioned safeguards and/or other information security practices as they pertain to the protection of Company's PHI, as Company may from time to time request. Upon reasonable advance request, Business Associate shall provide WellPoint access to Business Associate's facilities used for the maintenance or processing of PHI, and to its books, records, practices, policies and procedures concerning the Use and Disclosure of PHI, in order to determine Business Associate's compliance with this Agreement.

B. PHI Access, Amendment and Disclosure Accounting.

1. **Access.** Business Associate will promptly upon Company's request make available to Company or, at Company's direction, to the Individual (or the Individual's Personal Representative) for inspection and obtaining copies any PHI about the Individual which Business Associate created or received for or from Company and that is in Business Associate's custody or control, so that Company may meet its access obligations pursuant to and required by applicable law, including but not limited to 45 C.F.R. 164.524, and where applicable, the HITECH Act. Business Associate shall make such information available in electronic format where directed by the organization.

2. **Amendment**. Business Associate will, upon receipt of notice from Company, promptly amend or permit Company access to amend any portion of the PHI which Business Associate created or received for or from Company, pursuant to and required by applicable law, including but not limited to 45 C.F.R. Part 164.526.

   Business Associate will not respond directly to an Individual's request for an amendment of their PHI held in the Business Associate's Designated Record Set. Business Associate will refer the Individual to Company so that Company can coordinate and prepare a timely response to the Individual.

3. **Disclosure Accounting.** So that Company may meet its Disclosure accounting obligations pursuant to and required by applicable law, including but not limited to 45 C.F.R. Part 164.528:

   a) Disclosure Tracking. Business Associate will promptly, but no later than within seven (7) days of the Disclosure, report to Company for each Disclosure, not excepted from Disclosure accounting under Section B.3(b) below, that Business Associate makes to Company or a third party of PHI that Business Associate creates or receives for or from Company, (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 Company) 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 further shall provide any additional information, to the extent required by the HITECH Act or any regulation adopted pursuant thereto.

   b) Exceptions from Disclosure Tracking. Business Associate need not report Disclosure of information or otherwise account for Disclosures of PHI that this Agreement or Company in writing permits or requires (i) for the purpose of Company's Treatment activities, Payment activities, or Health Care Operations (except where such recording or accounting is required by the HITECH Act), and as of the effective dates for any such requirements, (ii) to the Individual who is the subject of the PHI disclosed, to that Individual's Personal Representative or to another person or entity authorized by the Individual (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, (vi) to Law Enforcement Officials or Correctional Institutions regarding Inmates; or (vii) disclosed in a limited data set.

      Business Associate need not report any Disclosure of PHI that was made before April 14, 2003.

   c) Except as provided below in subsection d) below, Business Associate will not respond directly to an Individual's request for an accounting of Disclosures. Business Associate will refer the Individual to Company so that Company can coordinate and prepare a timely accounting to the Individual.

   d) Disclosure through an Electronic Health Record. However, when Business Associate is contacted directly by an individual based on information provided to the individual by Company, Business Associate shall make the accounting of disclosures available directly to the individual, but only if required by the HITECH Act or any related regulations.

4. **Confidential Communications and Restriction Agreements**. Business Associate will promptly, upon receipt of notice from Company, send an Individual's communications to the identified alternate address. Business Associate will comply with any agreement Company makes that restricts Use or Disclosure of Company's PHI pursuant to 45 C.F.R. §164.522(a), provided that Company notifies Business Associate in writing of the restriction obligations that Business Associate must follow. Company will promptly notify Business Associate in writing of the termination or modification of any confidential communication requirement or restriction agreement.

5. **Disclosure to U.S. Department of Health and Human Services.** Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of PHI received from Company (or created or received by Business Associate on behalf of Company) available to the Secretary of the United States Department of Health and Human Services, for purposes of determining Company's compliance with 45 C.F.R. Parts 160-164. Unless the Secretary directs otherwise, Business Associate shall promptly notify Company of Business Associate's receipt of such request, so that Company can assist in compliance with that request.

C. Breach of Privacy and Security Obligations.

1. **Reporting.** Business Associate will report to Company: (i) any Use or Disclosure of PHI (including Security Incidents) not permitted by this Agreement or in writing by Company;(ii) any Security Incident; (iii) any Breach, as defined in the HITECH Act; or (iv) any other breach of a security system, or the like, as such may be defined under applicable state law (collectively a "Breach"). Except as described in subparagraph "e)" below, Business Associate will, without unreasonable delay, but no later than within one business day after Business Associate's discovery of a Breach, make the report by sending a report to Business Associate's assigned service support unit or by such other reasonable means of reporting as may be communicated to Business Associate by Company, after Business Associate discovers such Breach. Business Associate shall cooperate with Company in investigating the Breach and in meeting Company's obligations under the HITECH Act, and any other security breach notification laws or regulatory obligations.

   a) Report Contents. To the extent such information is available Business Associate's report will at least:

      (i) Identify the nature of the non-permitted or prohibited access, Use or Disclosure, including the date of the Breach and the date of discovery of the Breach;
      (ii) Identify the PHI accessed, used or disclosed, and provide an exact copy or replication of the PHI, as appropriate, in a format reasonably requested by Company, and to the extent available;
      (iii) Identify who caused the Breach and who received the PHI;
      (iv) Identify what corrective action Business Associate took or will take to prevent further Breaches;
      (v) Identify what Business Associate did or will do to mitigate any deleterious effect of the Breach; and
      (vi) Provide such other information, including a written report, as Company may reasonably request.

   b) Examples of Security Incidents. Company requires prompt notification from Business Associate if Business Associate experiences any Security Incidents that impact the confidentiality, integrity or availability of Company data or information systems. Below are some examples:
      (i) Business Associate's information systems are exposed to malicious code, such as a virus or worm, and such code could be transmitted to Company data or systems.
      (ii) Unauthorized access is granted or obtained to servers or workstations that contain Company data or Business Associate discovers that Company data is being used, copied, or destroyed inappropriately.
      (iii) Business Associate experiences an attack or the compromise of a server or workstation containing Company information requiring that it be taken offline.
      (iv) Unauthorized access or disclosure has occurred involving Protected Health Information, which is an obligation under the HIPAA Privacy Rule.

   c) Unsuccessful Security Incidents. Except as noted in C. 1 (e) below, the parties acknowledge and agree that this section constitutes notice by Business Associate to Company of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Company shall be required. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on

Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

d) Breach of Unsecured Protected Health Information. A Breach of Unsecured Protected Health Information includes any Breach as defined in the HITECH act or regulations adopted pursuant thereto.

e) Medicare Vendor Reporting Requirements –To the extent that Business Associate is subject to any Center for Medicare and Medicaid ("CMS") incident reporting requirements (including applicable timeframes for such reporting) as detailed in the services agreement between Company and Business Associate (including any amendments, exhibits or addenda), Business Associate shall comply with all such reporting requirements, in addition to those imposed hereby.

2. **Breach.** Without limiting the rights of the parties elsewhere set forth in the Agreement or available under applicable law, if Business Associate breaches its obligations under this Agreement, Company may, at its option:

a) Exercise any of its rights of access and inspection under paragraph 4 of section A of this Agreement

b) Require Business Associate to submit to a plan of monitoring and reporting, as Company may determine appropriate to maintain compliance with this Agreement and Company shall retain the right to report to the Secretary of HHS any failure by Business Associate to comply with such monitoring and reporting; or

c) Immediately and unilaterally, terminate the Agreement, without penalty to Company or recourse to Business Associate, and with or without an opportunity to cure the breach. Company's remedies under this Section and set forth elsewhere in this Agreement or in any other agreement between the parties shall be cumulative, and the exercise of any remedy shall not preclude the exercise of any other. If for any reason Company determines that Business Associate has breached the terms of this Agreement and such breach has not been cured, but Company determines that termination of the Agreement is not feasible, Organization may report such breach to the U.S. Department of Health and Human Services.

3. **Mitigation**. Business Associate agrees to mitigate to the extent practicable, any harmful effect that is known to Business Associate of any security incident related to PHI or any use or disclosure of PHI by Business Associate in violation of the requirements of this BA Agreement. To the extent Company incurs any expense Company reasonably determines to be necessary to mitigate any Breach or any other non-permitted use or disclosure of Individually Identifiable Information, Business Associate shall reimburse Company for such expense.

D. Compliance with Standard Transactions.

1. If Business Associate conducts in whole or part Standard Transactions, for or on behalf of Company, Business Associate will comply, and 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 for which HHS has established Standards. Business Associate will comply by a mutually agreed date, but no later than the date for compliance with all applicable final regulations, and will require any subcontractor or agent involved with the conduct of such Standard Transactions, to comply, with each applicable requirement of the Transaction Rule 45 C.F. R. Part 162. Business Associate agrees to demonstrate compliance with the Transactions by allowing Company 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 Company 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.

2. **Concurrence for Test Modification to Standard Transactions.** Business Associate agrees and understands that there exists the possibility that Company or others may request from HHS an exception from the uses of a Standard in the HHS Transaction Standards. If this request is granted by HHS, Business Associate agrees that it will participate in such test modification.

3. **Incorporation of Modifications to Standard Transactions** Business Associate agrees and understands that from time-to-time, HHS may modify and set compliance dates for the Transaction Standards. Business Associate agrees to incorporate by reference into this Agreement any such modifications or changes.

4. **Code Set Retention (Only for Plans).** Both parties understand and agree to keep open code sets being processed or used in the Agreement for at least the current billing period or any appeal period, whichever is longer.

5. **Guidelines and Requirements.** Business Associate further agrees to comply with any guidelines or requirements adopted by Company consistent with the requirements of HIPAA and any regulations promulgated thereunder, governing the exchange of information between Business Associate and the Company.

E. Obligations upon Termination.

1. **Return or Destruction.** Upon termination, cancellation, expiration or other conclusion of the Agreement, Business Associate will if feasible return to Company or destroy all PHI, in whatever form or medium (including in any electronic medium under Business Associate's custody or control), that Business Associate created or received for or from Company, 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 30 days after the effective date of the termination, cancellation, expiration or other conclusion of Agreement. Business Associate will identify any PHI that Business Associate created or received for or from Company that cannot feasibly be returned to Company 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 and will otherwise continue to protect the security any PHI that is maintained pursuant to the security provisions of this Agreement for so long as the PHI is maintained. Within such 30 days, Business Associate will certify in writing to Company that such return or destruction has been completed, will deliver to Company 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.

2. **Continuing Privacy and Security Obligation.** Business Associate's obligation to protect the privacy and security of the PHI it created or received for or from Company will be continuous and survive termination, cancellation, expiration or other conclusion of this Agreement, so long as the data is maintained.

F. General Provisions.

1. **Definitions.** The capitalized terms in this Agreement have the meanings set out in 45 C.F.R. Parts 160-164, as it may be amended from time to time. As of the execution date of this Agreement, the following are some of the relevant definitions set out in the Code of Federal Regulations.

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

   b) Electronic Media means (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines. Private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

   c) Individual means the person who is the subject of Protected Health Information.

   d) Individually Identifiable Health Information means information that is a subset of Protected 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 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
         a) that identifies the Individual; or
         b) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

   e) Protected Health Information ("PHI") means any information without regard to its form or medium, gathered by Business Associate in connection with Business Associate's relationship with Covered Entity that identifies an individual or that otherwise would be defined as Protected Health Information under HIPAA. :

   f) Security Incident means an attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system, involving Protected Health Information that is created, received maintained or transmitted by or on behalf of Company in electronic form.

   g) Use means, with respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information with an entity that maintains such information.

2. **Amendment.** From time to time local, state or federal legislative bodies, boards, departments or agencies may enact or issue laws, rules, or regulations pertinent this Agreement. In such event, Business Associate agrees to immediately abide by all said pertinent laws, rules, or regulations and to cooperate with Company to carry out any responsibilities placed upon Company or Business Associate by said laws, rules, or regulations.

3. **Conflicts.** The terms and conditions of this Agreement will override and control any conflicting term or condition of any other agreement between the parties with respect to the subject matter herein. All non-conflicting terms and conditions of the said other agreement(s) remain in full force and effect.

4. **Owner of PHI.** Company is the exclusive owner of PHI generated or used under the terms of the Agreement.

5. **Subpoenas.** Business Associates agrees to relinquish to Company control over subpoenas Business Associates receives with regard to PHI belonging to Company.

6. **Disclosure of De-identified Data.** The process of converting PHI to De-identified Data (DID) is set forth in 45 C.F.R Part 164.514. In the event that Company provides Business Associate with DID, Business Associate shall not be given access to, nor shall Business Associate attempt to develop on its own, any keys or codes that can be used to re-identify the data. Business Associate shall only use DID as directed by Company.

7. **Creation of De-identified Data.** In the event Business Associate wishes to convert PHI to DID, it must first subject its proposed plan for accomplishing the conversion to Company for Company's approval, which shall not be unreasonably withheld provided such conversion meets the requirements of 45 C.F.R. Part 164.514. Business Associate may only use DID as directed or otherwise agreed to by Company.

8. **Assignment/Subcontract.** Company shall have the right to review and approve any proposed assignment or subcontracting of Business Associate's duties and responsibilities arising under the Agreement, as it relates to the Use or creation of PHI (or DID if applicable].

9. **Audit.** Company shall have the right to audit and monitor all applicable activities and records of Business Associate to determine Business Associate's compliance with the requirements relating to the creation or Use of PHI [and DID, if applicable] as it relates to the privacy and security sections of this Agreement.

10. **Intent.** The parties agree that there are no intended third party beneficiaries under this Agreement.

11. **Branding**. Business Associate understands and agrees that Business Associate may not use the WellPoint name or brand with the Blue names or brands in the implementation of this Agreement

12. **Indemnity.** Business Associate will indemnify and hold harmless Company and any Company affiliate, officer, director, employee or agent from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any non-permitted or prohibited Use or Disclosure of PHI or other breach of this Agreement by Business Associate or any subcontractor, agent, person or entity under Business Associate's control.

    a) Right to Tender or Undertake Defense. If Company is named a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted or prohibited Use or Disclosure of PHI or other breach of this Agreement by Business Associate or any subcontractor, agent, person or entity under Business Associate's control, Company will have the option at any time either (i) to tender its defense to Business Associate, in which case

Business Associate will provide qualified attorneys, consultants and other appropriate professionals to represent Company's interests at Business Associate's expense, or (ii) undertake its own defense, choosing the attorneys, consultants and other appropriate professionals to represent its interests, in which case Business Associate will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants and other professionals.

b) Right to Control Resolution. Company will have the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that Company may have tendered its defense to Business Associate. Any such resolution will not relieve Business Associate of its obligation to indemnify Company under Section F.11 of this Agreement.

END OF AGREEMENT