BUSINESS ASSOCIATE AGREEMENT

If, during the term of any Agreement between Supplier and HealthSun Health Plans, Inc., Anthem, Inc. and/or any of its affiliates (collectively, "Covered Entity"), Supplier requires the use or disclosure of Protected Health Information, including creating, receiving, maintaining, or transmitting Protected Health Information, then Supplier shall be deemed a Business Associate of Covered Entity and the following provisions shall apply:

This agreement ("Agreement") shall be effective on the date of Supplier's signature and is between the Supplier ("Business Associate") identified in this Agreement and Covered Entity on behalf of itself and its affiliates 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 160-164, including Subpart E of 45 CFR Part 164), 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.

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, or disclose PHI it creates or receives for or from Company (or another business associate of Company), consistent with the Privacy Rule, the Security 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/or agents that create, receive, maintain, or transmit such PHI 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 use appropriate safeguards to comply with Subpart C of 45 CFR Part 164 and 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 Required Information Security Controls document attached hereto as Exhibit A and

incorporated herein. 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 privacy or security law.

During the term of this Agreement, Business Associate may be asked to complete a security survey and/or attestation document designed to assist Covered Entity in understanding and documenting Business Associate's security procedures and compliance with the requirements contained herein. Business Associate's failure to complete either of these documents within the reasonable timeframe specified by Covered Entity shall constitute a material breach of this Agreement

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 Covered Entity 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.

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 Company. Such report will be made on a form made available to Business Associate, or by such other reasonable means of reporting as may be communicated to Business Associate by Company. 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.(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 this Agreement and/or any other agreements between the parties, without penalty to Company, 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 is not curable or if curable, has not been cured, but Company determines that termination of this Agreement and/or any other agreements between the parties 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 shall destroy all PHI in accordance with any guidance set forth by the Secretary of HHS and/or any other government agency or other entity to whom HHS delegates such authority 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.** Except as otherwise provided, the capitalized terms in this Agreement have the meanings set out in 45 C.F.R. Parts 160-164, as may be amended from time to time. The term Protected Health Information ("PHI") includes 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

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. **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.

IN WITNESS WHEREOF, Company and Business Associate execute this Agreement in multiple originals to be effective on the date of Business Associate's Signature below:

Name of Business Associate	*Name of Company*
By: _____	*By:* _____
Signature	*Signature*
Printed Name	*Printed Name*
Title	*Title*
Date	*Date*

Business Associate Agreement - Exhibit A
Required Information Security Controls

Covered Entity requires all third parties to comply with the goals and objectives of its Information Security Program, as set forth in this addendum. These are minimum requirements of Covered Entity's Information Security Program. Depending upon the nature of the engagement or the services provided, other requirements may be added in a Statement of Work or Master Services Agreement. These requirements are in addition to any other security requirements specified within the Master Services Agreement or a Statement of Work. We recognize that sound practices require continual assessment of evolving risks, technology and relevant issues related to information security. In the event that our Chief Information Security Officer deems it necessary to modify these Required Information Security Controls in order to continue to reasonably protect Covered Entity Confidential Information, then Supplier will be notified and a remediation plan and timeframe will be mutually agreed upon.

1 Compliance

1.1 Supplier will comply with all applicable state and federal data security regulations and shall abide by all required security controls as stated herein, based upon the nature of the Services provided, the data involved and/or the location where such Services are rendered.

2 Information Security Program

2.1 Supplier shall maintain a written Information Security Program including documented policies, standards, and operational practices that meet or exceed the applicable requirements, and controls set forth in this Exhibit to the extent applicable to the Services, and identify an individual within the organization responsible for its enforcement. Supplier shall ensure that any of its subcontractors having greater than incidental access to Covered Entity Confidential Information shall also be contractually bound to meet or exceed these information security provisions. Supplier shall have processes and procedure in place so that information security events may be reported through appropriate communications channels as quickly as possible. All employees, contractors and third party users shall be made aware of their responsibility to report any information security events as quickly as possible. If at any time during the Agreement, Supplier becomes aware of an information security event or that it or any of its subcontractors will or do not meet the obligations described within this Exhibit, Supplier will immediately notify Covered Entity Information Security at AnthemVendorInfoSec@anthem.com.

3 Right to Assess, Audit and Certification

3.1 Upon request, Supplier shall complete a security assessment conducted by Covered Entity ("Security Assessment") Covered Entity may require additional Security Assessments in connection with Statements of Work for new or additional Services. To the extent that the Security Assessment identifies any risks or deficiencies for which remediation is required, such remediation requirements or compensating controls (and the timeframes within which they must be successfully implemented) are set forth in an attachment to this exhibit or the applicable Statement of Work. Supplier's failure to complete any remediation requirements set forth in an attachment to this exhibit or the applicable Statement of Work within the required timeframe shall be deemed to be a material breach of the Agreement. If Supplier has a Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) Certification applicable to the services and/or applications in scope for the engagement as of the Effective Date and maintains it throughout the engagement, then that HITRUST certification will be accepted in lieu of the Covered Entity assessment.

3.2 Supplier shall have, as of the Effective Date, and shall maintain for the duration of the engagement a HITRUST CSF Certification. To the extent that Supplier does not have a HITRUST

CSF Certification as of the Effective Date, or is the process of obtaining a HITRUST CSF Certification, the requirements of Section 3.3, as applicable, shall apply.

3.3 To the extent that Supplier has not obtained a HITRUST CSF Certification, then (a) the requirements of Section 3.4 shall apply, and (b) Supplier shall (i) complete and provide to Covered Entity a HITRUST CSF Self-Assessment Report 90 days after the Effective Date, (ii) obtain and provide to Covered Entity a HITRUST CSF Validated Report 18 months after the Effective Date,, and (iii) obtain and provide to Covered Entity a HITRUST CSF 24 months after the Effective Date, Supplier's failure to meet the foregoing requirements shall be deemed a material breach of the Agreement. If Supplier has begun the process of obtaining a HITRUST CSF Certification before the Effective Date, then Supplier represents and warrants to Covered Entity that all corrective action plans that are necessary to obtain a HITRUST CSF Validated Report and/or HITRUST CSF Certification and that have been identified to Supplier prior to the Effective Date shall be communicated to Covered Entity and documented as an attachment to this exhibit.

3.4 Supplier shall promptly (and in any event with 30 days of identification) report to Covered Entity Information Security at AnthemVendorInfoSec@anthem.com any findings and associated corrective action plans identified during a self-assessment or any third party assessment, including any assessment related to Supplier's Independent Certification / Attestation. Supplier will provide Covered Entity with any further information associated with such findings, as reasonably requested by Covered Entity.

3.5 From time to time Supplier may be requested to respond to, inform and provide updates on the specific security gaps or exposures that exist for new or emerging security vulnerabilities that are made known for systems, applications, hardware devices, etc. In all instances Supplier will provide a response to any inquiry within 5 business days, and will provide specific details as to the questions asked to ensure that Covered Entity can appropriately evaluate the risk or exposure to Covered Entity Confidential Information.

4 Encryption

4.1 Where required by Covered Entity, Supplier shall apply encryption methodology that conforms to the Federal Information Processing Standards Publication 140-2 Security Requirements for Cryptographic Modules and applicable state and federal regulations ("Approved Encryption"). Approved Encryption must be used for (i) the electronic transmission of Covered Entity Confidential Information to Covered Entity and/or to any other third party, as directed by Covered Entity or permitted in accordance with this Agreement and (ii) on all workstations, communications or convergence devices, portable media and backup tapes containing Covered Entity Confidential Information. The integrity and confidentiality of Covered Entity Confidential Information in transit over an open communication network will be protected through the use of Approved Encryption.

5 Network and Systems Security

5.1 Supplier shall utilize and maintain a commercially available, industry standard malware detection program which includes an automatic update function to ensure detection of new malware threats.

5.2 An Intrusion Detection or Prevention System which detects and/or prevents unauthorized activity traversing the network will be maintained.

5.3 Data Loss Prevention tools will be implemented to detect and prevent the unauthorized movement of data from Supplier's control.

5.4 At a minimum, Supplier shall engage a qualified third party to perform annual penetration testing of Supplier's networks containing Covered Entity Confidential Information. The scope of the penetration testing will include all internal/external systems, devices and applications that are used to process, store, transmit Confidential Data, physical security controls for all applicable facilities, and social engineering tests. Supplier must provide Covered Entity with summary results and a remediation plan if security flaws are discovered.

5.5 Networks or applications that contain Covered Entity Confidential Information must be separated from public networks by a firewall to prevent unauthorized access from the public network.

5.6 At managed interfaces, network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception).

6 System and Application Controls

6.1 All Covered Entity Confidential Information must be securely stored at all times to prevent loss and unauthorized access or disclosure.

6.2 Laptop and workstation systems that access Covered Entity Confidential Information remotely must utilize endpoint protection which includes a personal firewall and anti-malware protection.

6.3 Operating systems and application software used must be currently supported by the manufacturer.

6.4 Current versions of operating system and application software must be maintained, and patches applied in a timely manner for all systems and applications that receive, maintain, process or otherwise access Covered Entity Confidential Information.

6.5 At least quarterly vulnerability scanning will be performed. Medium and high risk vulnerabilities identified during the scanning will be promptly remediated.

6.6 Covered Entity Confidential Information must not be used in any non-production environment such as testing or quality assurance unless de-identification of the data has been performed. In the event that de-identification is not practical or feasible compensating controls must be in place protecting the data to the same level of protection as afforded to production environment.

6.7 Covered Entity Confidential Information must be logically or physically segregated from other data controlled by Supplier or other clients of Supplier in such a way that the data may be identified as Covered Entity data and access controls implemented so that only those users authorized to access the data will be permitted to do so.

7 Data Destruction

7.1 All Covered Entity Confidential Information, whether such information is in paper, electronic or other form, requires secure disposal or destruction when no longer required, when requested by Covered Entity or upon the termination or expiration of the Agreement. These measures should, at a minimum, include: (i) burning, pulverizing or cross-cut shredding to a size equal or smaller to 5/8- inch by 2-inches papers or print media so that the information cannot practicably be read or reconstructed; (ii) ensuring the destruction or erasure of floppy disk, magnetic tape, tape cartridges, hard drives or other electronic or optical media so that the information recorded or contained cannot practicably be read, recovered or reconstructed; and, (iii) ensuring that any third party who performs the activities described in (i) and (ii) on

Supplier's behalf does so in a manner consistent with these requirements.

8 Physical Controls for the Protection of Covered Entity Confidential Information

8.1 All Covered Entity Confidential Information received or created in paper form must be stored in lockable containers.

8.2 A clean desk policy will be enforced to ensure proper safeguarding of all hard copy Covered Entity Confidential Information.

8.3 Supplier must retain visitor logs documenting all individuals who are not employed by Supplier who gain access to the facility where services are performed.

8.4 Covered Entity Confidential Information will not leave control of the Supplier without the written approval of Covered Entity.

8.5 Servers, enterprise data storage devices, backup tapes and media, and other computing devices that contain Covered Entity Confidential Information used to support network communications must be located in a secure and restricted access location within the facility.

8.6 All workstations, portable devices and removable media containing Covered Entity Confidential Information or accessing Covered Entity networks must be encrypted.

9 Access Control

9.1 Prior to gaining access to Covered Entity Confidential Information, workforce members will have appropriate background checks completed in compliance with state and federal law with no breach of trust crimes reported.

9.2 Physical and logical access to Covered Entity Confidential Information and the systems and workspaces used to support Covered Entity, will only be granted as a result of a demonstrated and legitimate need to know based upon job responsibilities.

9.3 Security awareness training will be completed prior to access being granted to Covered Entity Confidential Information, and then completed on an annual basis going forward so long as access to Covered Entity Confidential Information continues.

9.4 Physical and logical access will be granted to the minimum Covered Entity Confidential Information necessary to meet the requirements of the user's scope of responsibilities.

9.5 Access reviews will be performed at least quarterly for privileged user and twice annually for non- privileged user accounts.

9.6 Only those individuals providing services to Covered Entity, or those who are responsible for administering or managing systems that contain Covered Entity Confidential Information shall be authorized to access systems containing Covered Entity Confidential Information.

9.7 All users that are no longer required or authorized to access Covered Entity Confidential Information or systems that contain Covered Entity Confidential Information must have access promptly disabled.

9.8 Access to Covered Entity Confidential Information and systems that contain Covered Entity Confidential Information must be access controlled through the use of individual user IDs and passwords with industry-standard complexity rules in place.

9.9 All user passwords must be changed at least every ninety (90) days at a minimum, or sooner if there is reasonable cause to believe that an unauthorized person has learned the password.

9.10 Processes must be in place to create the appropriate audit trails to determine who has accessed Covered Entity Confidential Information and/or systems that contain Covered Entity Confidential Information.

9.11 Remote access to systems or networks that contain Covered Entity Confidential Information must use multi-factor authentication and a connection with Approved Encryption.

9.12 A report listing all individuals who have access to Covered Entity Confidential Information and/or systems that contain Covered Entity Confidential Information and the level of access granted shall be provided to Covered Entity within 48 hours upon request.

9.13 A report listing activity associated with any user ID who has access to Covered Entity Confidential Information shall be provided to Covered Entity within 48 hours upon request.

10 Offshore Security Requirements

10.1 Covered Entity Confidential Information is not permitted to be hosted or stored offshore. Offshore locations may be utilized for the processing of data. However, all data must reside on servers located in the United States for the duration of the processing.

10.2 Backup processes at offshore locations will not receive, maintain, process, or otherwise access Covered Entity Confidential Information.

10.3 Offshore workstation computers must adhere to baseline system security requirements defined by the organization which enforce the most restrictive mode consistent with operational requirements. All unnecessary services, features and networks must be disabled on workstations used to support Covered Entity operations, including:

- Disabling workstations from simultaneously connecting to the Covered Entity network and other networks (split tunneling)
- Disabling access to non-Covered Entity instant messaging (IM) clients
- Disabling access to non-Covered Entity email systems
- Disabling access to the Internet
- Disabling user access to local workstation storage or supplier network storage (such as that to which Covered Entity Confidential Information or screenshots could be copied)
- Disabling access to printers

10.4 Wireless access is prohibited from being used to access Covered Entity Confidential Information from offshore locations.

10.5 All work from offshore locations must be performed in Covered Entity-approved facilities.

11 Cloud Computing

Covered Entity bases the decision of whether a service is considered a cloud based technology on

several factors including the five essential characteristics defined by the National Institute of Standards and Technology (NIST), Note that the absence of one or more of these characteristics is not viewed as a final deciding factor when determining if a service is Cloud based. Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

11.1 The use of a multi-tenant environment is prohibited for hosting Confidential Information, unless a risk assessment has been performed and the appropriate Covered Entity Information Security approved risk mitigating controls are in place.

11.2 Logical controls, virtual machine zoning, virtualization security and segregation must be in place to help prevent attacks and exposure in multi-tenancy environments.

11.3 Covered Entity Confidential Information must be segregated from non-Covered Entity Information so that appropriate controls are in place to identify the data as Covered Entity's in all instances, including backup and removable media, and to appropriately restrict access to only users authorized to view the data. Logical separation must allow data to be deleted when it is no longer required

11.4 Covered Entity Confidential Information included in a cloud computing-based environment must be protected with Covered Entity Approved Cryptographic Controls in transit, storage, and at rest. Appropriate Encryption key management must also be provided.

11.5 All Covered Entity data hosted in a cloud environment must remain on US-based systems and may not be stored outside of the United States.

11.6 The Cloud Service Provider (CSP) must provide a detailed mechanism for how litigation holds will be implemented. This will include how metadata will be created, accessed, and stored in the cloud environment.

11.7 Cloud Service Providers must undergo an annual independent audit by an accredited auditing firm covering the scope of Covered Entity data. Results of this audit must be provided to Covered Entity along with associated remediation decisions and activities, if applicable.

11.8 In the event Cloud Service Provider is not able to continue providing Services, then arrangements will be made for Covered Entity to receive its Confidential Information back from the CSP.

11.9 Incident response roles and responsibilities must be clearly outlined between the cloud service provider and Covered Entity or CSP and Supplier as appropriate.

11.10 Quarterly vulnerability scans must be performed, and intrusion detection and identity management systems must be installed on all systems and components that handle, process, or store Covered Entity data. Upon request, report summaries, including confirmation of remediation for vulnerabilities identified as high- or medium-risk, must be provided to Covered Entity Information Security.

11.11 When virtual machines or instances are no longer used, moved from one physical server to another, or have been decommissioned, all data must be zeroed or destroyed using Information Security approved techniques.

11.12 The CSP must be able to enforce the account management capabilities, such as account lockouts for unsuccessful logon attempts, defined inactivity times, remote access

allowances, specific success and failure events, and management of elevated privilege accounts.

11.13 All identity credentialing, authentication, authorization, and access control events must be logged and those logs are subject to periodic audit. At a minimum, the CSP must produce logs of all specified success and failure events associated with identity and access management in the cloud environment it manages. These logs must then be archived for at least twelve months. These archived logs must be searchable and or discoverable.

11.14 The CSP must conduct access reviews quarterly for privileged user accounts and twice yearly for non-privileged user accounts.

12 Enterprise Standards Governance

12.1 If upon review by Covered Entity's Enterprise Standards Governance, items are identified for remediation, such remediation must be completed in agreed upon timeframes.

13 Contingency Planning

13.1 Supplier will have documented Business Continuity and Disaster Recovery plans in place that include information security controls. Such plans will be tested at least annually.

14 Incident Response

14.1 Supplier will have documented Incident Response Plan. Such plan will be tested at least annually.

15 Payment Card Industry Data Security Standard

15.1 If, in performing services to or on behalf of Covered Entity, Supplier acts as a Merchant as defined by the Payment Card Industry Data Security (PCI DSS) standard, then Supplier agrees to comply with the applicable PCI DSS requirements.