

BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT ("Agreement") is effective the ____ day of _____, 20____ by and between _____ ("Business Associate") and AMERICAN NATIONAL INSURANCE COMPANY and subsidiaries AMERICAN NATIONAL LIFE INSURANCE COMPANY OF TEXAS, GARDEN STATE LIFE INSURANCE COMPANY and STANDARD LIFE AND ACCIDENT INSURANCE COMPANY ("the Companies")

Background

Companies are covered entities under the Health Insurance Portability and Accountability Act of 1996, as amended (the "Act"), the *Standards for privacy of Individually Identifiable Health Information* (the "Privacy Rule") and the *Security Standards for the Protection of Electronic Protected Health Information* (the "Rule"), promulgated under the Act (the Privacy Rule, Security Rule and the Act are collectively referred to herein as "HIPAA"). In addition, it is the intent of the parties to comply with the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") of the American Recovery and Reinvestment Act of 2009 ("ARRA"), Pub. L. 111-5, and its regulations.

Companies and Business Associate have entered into a business relationship pursuant to an agreement (the "Prime Agreement") under which, among other things, Companies may provide to Business Associate certain protected health information to enable the Business Associate to perform its obligations thereunder (the "Obligations").

In order for the Business Associate to perform its Obligations, the Privacy Rule and the Security Rule require that Companies obtain adequate assurances from Business Associate in the form of a written agreement that contains certain mandatory provisions regarding Business Associate's use and disclosure of protected health information (as defined in HIPAA) that is created or received for or from Companies in connection with Business Associate's performance of the Obligations ("Companies Protected Health Information").

NOW, THEREFORE, in consideration of the premises, the parties, intending to be legally bound, agree as follows

1. Privacy of Protected Health Information.

- a) Permitted Use. Business Associate is permitted to use and disclose Companies' Protected Health Information only:
 - i) in connection with its performance of the Obligations under the Prime Agreement, or
 - ii) for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities, provide that, with respect to disclose of Companies' Protected Health Information to a third party, either:
 - A) The disclosure is Required by Law; or
 - B) Business Associate obtains reasonable assurance from any person or entity to which business Associate will disclose Companies' Protected Health Information that the person or entity will:

- 1) hold Companies' Protected Health Information in confidence and use or further disclose Companies' Protected Health Information only for the purpose for which Business Associate disclosed Companies' Health Information to the person or entity or as Required by Law; and
 - 2) promptly notify Business Associate of any instance of which the person or entity becomes aware in which the confidentiality of Companies' Protected Health Information was breached.
- iii) Business Associate will make reasonable efforts to use, disclose, and request only the minimum amount of Companies' Protected Health Information reasonably necessary to accomplish the intended purpose, except that Business Associate will not be obligated to comply with this minimum necessary limitation if neither Business Associate nor Companies are required to limit the use, disclosure or request to the minimum necessary.
- b) Prohibition on Unauthorized Use or Disclosure. Business Associate will neither use nor disclose Companies' Protected Health Information, except as permitted or required by this Agreement or as permitted or directed by Companies or as Required by Law. This Agreement does not authorize Business Associate to use or disclose Companies' Protected Health Information in a manner that would violate the Privacy Rule or the HITECH Act if done by Companies, except as set forth in Section 1(a)(ii).
- c) Information Safeguards.
 - i) Business Associate will develop, implement, maintain, and use industry specific and/or other generally appropriate administrative, technical, and physical safeguards to protect Companies' Protected Health Information from any use or disclosure in violation of the Privacy Rule.
 - ii) Business Associate will develop, implement, maintain, and use industry specific and/or other generally appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of Electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on Companies' behalf as required by the Security Rule.
 - iii) The information safeguards must meet or exceed the industry specific and/or other generally appropriate minimum standards.
 - iv) If applicable and only if available, Business Associate will provide Companies a copy of the most recent SAS70 audit report.
- d) Subcontractors and Agents. Business Associate will require any of its subcontractors and agents, to which Business Associate is permitted to disclose Companies' Protected Health Information, to provide reasonable assurance that such subcontractor or agent will comply with the same privacy and security safeguard obligations with respect to Companies' Protected Health Information that are applicable to Business Associate under this Agreement.
- e) Prohibition on Sale of Records. Business Associate shall not directly or indirectly receive remuneration in exchange for any Companies' Protected Health Information of an individual unless the Company or Business Associate obtained from the individual a valid authorization that includes a specification of whether the Companies' Protected Health Information can be

further exchanged for remuneration by the entity receiving Companies' Protected Health Information of that individual, except as otherwise allowed under the American Recovery and Reinvestment Act.

2. Compliance with Transaction Standards. If Business Associate conducts in whole or part electronic Transactions on behalf of Companies for which the Department of Health and Human Services ("DHHS") has established Standards, Business Associate will comply, and will require any subcontractor or agent it involves with the conduct of such Transactions to comply, with each applicable requirement of the Transaction Rule, 45 C.F.R. Part 162. Business Associate shall comply with the National Provider Identifier requirements if, and to the extent, applicable.
3. Individual Rights.
 - a) Access. Business Associate will, within thirty calendar days following Companies' request, make available to Companies or, at Companies' direction, to an individual (or the individual's personal representative), for inspection and obtaining copies (at Companies' expense), Companies' Protected Health Information about the individual that is in Business Associate's custody or control. If the Companies' Protected Health Information is held in an Electronic Health Record, then the individual shall have a right to obtain from Business Associate a copy of such information in an electronic format. Business Associate shall provide such a copy to Companies or, alternatively, to the individual directly, if such alternative choice is clearly, conspicuously and specifically made by the individual or Companies.
 - b) Amendment. Business Associate will, upon receipt of written notice from Companies, promptly amend or permit Companies access to amend any portion of Companies Protected Health Information, so that Companies may meet amendment obligations under the Privacy Rule.
 - c) Disclosure Accounting. So that Companies may meet disclosure accounting obligations under the Privacy Rule:
 - i) Business Associate will record information specified in Section 3(c)(iii) below ("Disclosure Information") for each disclosure of Companies' Protected Health Information, not excepted from disclosure accounting as specified in Section 3(c)(ii) below, that Business Associate makes to Companies or to a third party.
 - ii) Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of Companies' Protected Health Information if the Company need not account for such disclosures.
 - iii) With respect to any disclosure by Business Associate of Companies' Protected Health Information that is not excepted from disclosure accounting by Section 3(c)(ii) above, Business Associate will record the following Disclosure Information as applicable to the type of accountable disclosure made:
 - A) For non-repetitive disclosures of Companies' Protected Health Information, the Disclosure Information that Business Associate must record for each accountable disclosure is (i) the disclosure date, (ii) the name and (if known) address of the entity to which Business Associate made the disclosure, (iii) a

brief description of Companies' Protected Health Information disclosed, and (iv) a brief statement of the purpose of the disclosure.

B) For repetitive disclosures of Companies' Protected Health Information that Business Associate makes to the same person or entity (including Companies), Business Associate may record either (1) the Disclosure Information specified above for each accountable disclosure, or (2) the Disclosure Information specified in Section 3(c)(iii)(A) above for periodicity, or number of the repetitive accountable disclosures, and the date of the last of the repetitive accountable disclosures during the Accounting Period.

iv) Business Associate will maintain the Disclosure Information for at least 6 years following the date of the disclosure (3 years for disclosures related to an Electronic Health Record).

Business Associate will make the Disclosure Information available to Companies within sixty calendar days following Companies' request for such Disclosure Information to comply with an individual's request for disclosing accounting. With respect to disclosures related to an Electronic Health Record, Business Associate shall provide the accounting directly to an individual making such a disclosure request, if a direct response is requested by the individual. Notwithstanding any other provision of this Agreement, Business Associate needs to provide disclosure accounting related to an Electronic Health Record only as of the effective date of this requirement under the American Recovery and Reinvestment Act.

d) Restriction Agreements and Confidential Communications. Business Associate will comply with any agreement that Companies make that either (i) restricts use or disclosure of Companies' Protected Health Information or requires confidential communication about Companies' Protected Health Information, provided that Companies notify Associate in writing of the restriction or confidential communication obligations that Business Associate must follow. Companies 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 whether any of Companies' Protected Health Information will remain subject to the terms of the restriction agreement. Effective February 17, 2010 (or such other date specified as the effective date by DHHS), Business Associate will comply with any restriction request if: (i) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (ii) the Protected Health Information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

4. Privacy Obligation Breach and Security Incidents.

a) Reporting.

(i) Business Associate will report to Companies any use or disclosure of Companies' Protected Health Information not permitted by this Agreement or in writing by Companies, along with any Breach of Unsecured Company Protected Health Information. Business Associate will treat the Breach as being

Discovered in accordance with HIPAA's requirements. Business Associate will make the report to Companies' Privacy Official not more than sixty calendar days after Business Associate learns of such non-permitted use or disclosure. If a delay is requested by law enforcement official in accordance with 45 C.F.R. § 164.412, Business Associate may delay notifying Organization for the time period specified by such regulation. Business Associate's report will at least:

- A) Identify the nature of the Breach or other non-permitted use or disclosure, which will include a brief description of what happened, including the date of any Breach and the date of the discovery of any Breach;
- B) Identify Companies' Protected Health Information that was subject to the Breach or other non-permitted use or disclosure, including, if applicable, the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired or disclosed during such Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- C) Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;
- D) Identify what corrective action Business Associate took or will take to prevent further non-permitted uses or disclosures, to mitigate losses and to protect against any further Breaches;
- E) Identify what steps the individuals who were subject to a Breach should take to protect themselves from potential harm resulting from the breach;
- F) Provide such other information, including a written report, as Companies may reasonably request.

- v) Business Associate will report to Companies within thirty calendar days any attempt or successful (A) unauthorized access, use, disclosure, modification or destruction of Companies' Electronic Protected Health Information or (B) interference with Business Associate's system operations in Business Associate's information systems, of which Business Associate becomes aware. Business Associate will make this report upon Companies' request, except if any such security incident resulted in a disclosure or Breach of Companies' Protected Health Information or Electronic Protected Health Information not permitted by this Agreement, Business Associate will make the report in accordance with Section 4(a)(i) above.

b) Termination of Agreement.

- i) Companies may terminate this Agreement if they determine, in their sole discretion, that Business Associate has breached a material term of this Agreement and, upon written notice to Business Associate of the breach, Business Associate fails to cure the breach within thirty calendar days. Companies may exercise this right to terminate by providing Business Associate written notice of termination, stating the failure to cure the breach of the Agreement that provides the basis for the

termination. Any such termination will be effective immediately or at such other date specified in Companies' notice of termination.

- ii) Either the Companies or Business Associate may terminate this Agreement if amendment or addition to 45 C.F.R Parts 160-64 affects the obligations under this Agreement of the party exercising the right of termination. The party so affected may terminate this Agreement by giving the other party written notice of such termination at least 90 calendar days before the compliance date of such amendment or addition to 45 C.F.R Parts 160-64.

iii) Obligations on Termination.

- A) Upon termination or other conclusion of this Agreement, Business Associate will, if feasible, return to Companies or destroy all of Companies' Protected Health Information in whatever form or medium. Business Associate will require any subcontractor or agent, to which Business Associate has disclosed Companies' Protected Health Information as permitted by Section 1(e) of this Agreement, to if feasible return to Business Associate (so that Business Associate may return it to Companies) or destroy all of Companies' Protected Health Information in whatever form or medium held by Business Associate. Business Associate will complete these obligations no later than sixty calendar days following the effective date of the termination or other conclusion of this Agreement.
- B) Business Associate will identify any of Companies' Protected Health Information, including any that Business Associate has disclosed to subcontractors or agents as permitted by Section 1(e) of this Agreement, that cannot feasibly be returned to Companies or destroyed and explain why return or destruction is infeasible. Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. Business Associate will require such subcontractor or agent to limit its further use or disclosure of Companies' Protected Health Information that such subcontractor or agent cannot feasibly return or destroy to those purposes that make the return or destruction of such information infeasible. Business Associate will complete these obligations no later than sixty calendar days following the effective date of the termination or other conclusive of this Agreement.
- C) Business Associate's obligation to protect the privacy and safeguard the security of Companies Protected Health Information as specified in the Agreement will be continuous and survive termination or other conclusion of this Agreement.

5. General Provisions.

- a) Inspection of Internal Security Capabilities, Practices, Books and Records. Business Associate will make its internal security capabilities, practices, books, and records relating to its use, disclosure and security of Companies' Protected Health Information available to Companies and to the DHHS to determine Companies' compliance with the Privacy and Security Rules.

- b) Business Associate External Access to Company Systems. Should the nature of Business Associate's contract with the Companies require Business Associate to access Companies' systems and data, there will be no sharing or pooling of logins associated with the Business Associate's access. In no event shall Companies' Protected Health Information be downloaded to personal storage devices of any type for any purpose.
- c) Definitions. All capitalized terms that are used but not otherwise defined in this Agreement shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance. For purposes of this Agreement, Companies' Protected Health Information encompasses Companies' Electronic Protected Health Information.
- d) Amendment to Agreement. Upon the effective date of any final regulation or amendment of final regulation promulgated by the DHHS that affects Business Associate's use or disclosure of Companies' Protected Health Information, this Agreement will automatically be deemed amended such that the obligations imposed on Business Associate remain in compliance with the final regulation or amendment to final regulation, unless Companies or Business Associate elects to terminate Agreement in accordance with Section 4(b)(ii).
- e) No Third Party Beneficiaries. Nothing in this Agreement shall be construed as creating any rights or benefits to any third parties.
- f) Prior Agreement Terminated. This Agreement supersedes any prior agreement of the parties concerning similar subject matter, and such prior agreement is hereby terminated.

IN WITNESS WHEREOF, Companies and Business Associate have executed this Agreement the day and year first above mentioned.

BUSINESS ASSOCIATE

THE COMPANIES

By: _____

By: _____

William J. Hogan
AVP- Group Health & HIPAA
Compliance

Title: _____