**COMBINED HIPAA PRIVACY BUSINESS ASSOCIATE AGREEMENT AND CONFIDENTIALITY AGREEMENT AND HIPAA SECURITY RULE ADDENDUM AND HITECH ACT COMPLIANCE AGREEMENT**

The parties have entered into this Agreement for the purpose of satisfying the Business Associate contract requirements of the regulations at 45 CFR 164.502(e) and 164.504(e), issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Security Rule, codified at 45 Code of Federal Regulations ("C.F.R.") Part 164, Subparts A and C., the Health Information Technology For Economic and Clinical Health Act (the HITECH Act, as enacted in Pub. L. No. 111-05 H.R., 111th Cong. (2009), Title XIII.), as well as the confidentiality requirements contained in section 110.123 (9), Florida Statutes.

Term: This Agreement shall be effective as of [ ], and shall terminate on as set forth herein.

**1.0 Definitions**

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 CFR 160.103; 164.105; 164.402; and 164.501; 164.502; 164.520 and in the HITECH Act, Subtitle D. Those terms include but are not limited to: Breach, Data, Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual Minimum Necessary, Notice of Privacy Practices, Required by Law, Secretary, Subcontractor, Unsecured Protected Health Information, and Use.

**Specific Definitions**

"Agency" means the Department of Management Services, an executive agency of the State of Florida, and its Division of State Group Insurance with its principle place of business at 4050 Esplanade Way, Suite 215, Tallahassee, FL 32399-0950.

"Business Associate" [ ] with a place of business at [ ].

"Contract" means the document that contains the terms and conditions for any services to be provided by the Business Associate to the Covered Entity effective as of[ ] and terminating on [ ].

"Covered Entity" means the State of Florida's Division of State Group Insurance (DSGI).

"HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at CFR Part 160 and Part 164.

"Individual" has the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

"Parties" mean collectively the Agency and the Business Associate. A "party" means either the Agency or the Business Associate.

"Plans" means the insurance coverages offered through the Covered Entity, as authorized in section 110.123, Florida Statutes.

"Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

"Protected Health Information" is defined in HIPAA at 45 CFR 160.103, and as used in this Agreement also refers to the term "Protected Health Information," as defined in the HITECH Act.

"Secretary" means the Secretary of the U.S. Department of Health and Human Services or designee.

"Security Incident" means any event resulting in computer systems, networks, or data being accessed, viewed, manipulated, damaged, destroyed or made inaccessible by an unauthorized activity. See National Institute of Standards and Technology (NIST) Special Publication 800-61, "Computer Security Incident Handling Guide," for more information.

**Part I – Privacy Provisions**

**2.0 Obligations and Activities of Business Associate**

**Business Associate Agrees to:**

(a) Not use or further disclose Protected Health Information other than as permitted or required by Sections 3.0, 5.0 and 6.0 of this Agreement, or as required by applicable federal or laws of the state

(b) Use appropriate safeguards, and comply with Subpart C 45 CFR 164 with respect to electronic Protected Health Information to prevent use or disclosure of the Protected Health other than as provided for by this Agreement.

(c) Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(d) Report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware, including Breaches of unsecured Protected Health Information as required by 45 CFR 164.410 and any security Incident of which it become aware.

(e) Ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) Provide access, at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations, to Protected Health Information in a designated record set, to the Covered Entity or directly to an Individual in order to meet the requirements under 45 CFR 164.524.

(g) Make any Amendment(s) to Protected Health Information in a designated record set that the Covered Entity or an Individual directs or agrees to pursuant to 45 CFR 164.526, in a prompt and reasonable manner consistent with the HIPAA regulations, or take other measures as necessary to satisfy Covered Entity obligation under 45 CFR 164.526.

(h) Make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(i) Document disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(j) At Covered Entity's or Individual's request, Business Associate agrees to provide to Individual or Covered Entity an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528, in a prompt and reasonable manner consistent with the HIPAA regulations. The Business Associate shall

assist the Covered Entity in complying with the HIPAA regulations relating to the required Disclosure, Amendment or Accounting.

(k) Business Associate certifies that it is in compliance with all applicable provisions of HIPAA standards for electronic transactions and code sets, also known as the Electronic Data Interchange (EDI) Standards, at 45 CFR Part 162; and the Annual Guidance as issued by the Secretary pursuant to the HITECH Act, sec. 13401.Business Associate further agrees to ensure that any agent, including a subcontractor, that conducts standard transactions on its behalf, agrees to comply with the EDI Standards and the Annual Guidance.

(l) Business Associate agrees to determine the Minimum Necessary type and amount of PHI required to perform its services and will comply with 45 CFR 164.502(b) and 164.514(d).

**3.0 Permitted or Required Uses and Disclosures by Business Associate**

General Use and Disclosure.

(a) Except as expressly permitted in writing by DMS/ DSGI, Business Associate shall not divulge, disclose, or communicate protected health information to any third party for any purpose not in conformity with this Contract without prior written approval from the Covered Entity.

(b) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide data aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).

(c) Business Associate may use and disclose Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j) (1).

(d) Business Associate may use and/or disclose Protected Health Information for Business Associate's proper management and administration, provided that: (i) Business Associate obtains reasonable assurances from the person whom Protected Health Information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person; and (ii) the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health information has been breached. Business Associate also may make disclosures that are Required By Law. The Business Associate's use of Protected Health Information as described in this paragraph is subject to and limited as described in 45 CFR 164.504(e)(2) and (4).

(e) Business Associate may create a Limited Data Set only as necessary and required for the purpose of performing its obligations and services for Covered Entity, provided that Business Associate complies with the provisions of this Agreement.

**4.0. Obligations of Covered Entity to Inform Business Associate of Covered Entity's Privacy Practices, and any Authorization or Restrictions.**

(a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, Authorization by Individual or his or her personal representative to use or disclose Protected Health Information, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, if such changes affect Business Associate's uses or disclosures of Protected Health Information

**5.0 Confidentiality Under State Law**

(a) In addition to the HIPAA privacy requirements, Business Associate agrees to observe the confidentiality requirements of section 110.123 (9), Florida Statutes. In general, the referenced statute provides that patient medical records and medical claims records of state employees, former state employees, and their covered dependents are confidential and exempt from the provisions of section 119.07 (1), Florida Statutes, known as the public records law of the State of Florida. Any person who willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation, including those residing or existing internal and external to the DMS/DSGI computer system, commits an offense in violation of section 815.04, Florida Statutes.

Confidentiality requirements protect more than unlawful disclosure of documents. The confidentiality requirements protect the disclosure of all records and information of DMS/DSGI, in whatever form, including the copying or verbally relaying of confidential information.

(b) Receipt of a Subpoena. If Business Associate is served with subpoena requiring the production of DMS/DSGI records or information, Business Associate shall immediately contact the Department of Management Services, Office of the General Counsel, (850) 487-1082.

A subpoena is an official summons issued by a court or an administrative tribunal, which requires the recipient to do one or more of the following:

a. Appear at a deposition to give sworn testimony, and may also require that certain records be brought to be examined as evidence.

b. Appear at a hearing or trial to give evidence as a witness, and may also require that certain records be brought to be examined as evidence.

c. Furnish certain records for examination, by mail or by hand-delivery.

(c) Employees and Agents. Business Associate acknowledges that the confidentiality requirements herein apply to all its employees, agents and representatives and subcontractors. Business Associate assumes responsibility and liability for any damages or claims, including state and federal administrative proceedings and sanctions, against DMS/DSGI, including costs and attorneys' fees, resulting from the breach by Business Associate of the confidentiality requirements of this Agreement.

**6.0 Permissible Requests by Covered Entity.**

(a) Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under HIPAA, the Privacy Rule, the HITECH Act and of the laws of the State of Florida, if done by Covered Entity.

(b) Covered Entity shall not provide Business Associate with more Protected Health Information than that which is minimally necessary for Business Associate to provide the services and, where possible, Covered Entity shall provide any Protected Health Information needed by Business Associate to perform the services in the form of a Limited Data Set, in accordance with the HIPAA regulations.

**7.0 Termination**

(a) *Protected Health Information*. Prior to the termination of this Agreement, the Business Associate shall destroy or return to the Covered Entity all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity. If it is infeasible or impossible to return or destroy Protected Health Information, the Business Associate shall immediately inform the Covered Entity of that and the parties shall cooperate in securing the destruction of Protected Health Information, or its return to the Covered Entity. Pending the destruction or return of the Protected Health

Information to the Covered Entity, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) *Termination for Cause.* Without limiting any other termination rights the parties may have, upon Covered Entity's knowledge of a material breach by Business Associate of a provision under this Agreement, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation. If the Agreement of Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, the Covered Entity shall have the right to immediately terminate the Agreement. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(c) *Effect of Termination.* Within sixty (60) days after termination of the Agreement for any reason, or within such other time period as mutually agreed upon in writing by the parties, Business Associate shall return to Covered Entity or destroy all Protected Health Information maintained by Business Associate in any form and shall retain no copies thereof. Business Associate also shall recover, and shall return or destroy with such time period, any Protected Health Information in the possession of its subcontractors or agents. Within fifteen (15) days after termination of the Agreement for any reason, Business Associate shall notify Covered Entity in writing as to whether Business Associate elects to return or destroy such Protected Health Information, or otherwise as set forth in this Section 7.0(c). If Business Associate elects to destroy such Protected Health Information, it shall certify to Covered Entity in writing when and that such Protected Health Information has been destroyed. If any subcontractors or agents of the Business Associate elect to destroy the Protected Health Information, Business Associate will require such subcontractors or agents to certify to Business Associate and to Covered Entity in writing when such Protected Health Information has been destroyed. If it is not feasible for Business Associate to return or destroy any of said Protected Health Information, Business Associate shall notify Covered Entity in writing that Business Associate has determined that it is not feasible to return or destroy the Protected Health Information and the specific reasons for such determination. Business Associate further agrees to extend any and all protections, limitations, and restrictions set forth in this Agreement to Business Associate's use or disclosure of any Protected Health Information retained after the termination of this Agreement, and to limit any further uses or disclosures to the purposes that make the return or destruction of the Protected Health Information not feasible. If its not feasible for Business Associate to obtain, from a subcontractor or agent, any Protected Health Information in the possession of the subcontractor or agent, Business Associate shall provide a written explanation to Covered Entity and require the subcontractors and agents to agree to extend any and all protections, limitations, and restrictions set forth in this Agreement to the subcontractors' or agents' uses or disclosures of any Protected Health Information retained after the termination of this Agreement, and to limit any further uses or disclosures to the purposes that make the return or destruction of the Protected Health Information not feasible.

**Part II – Security Addendum**

**8.0 Security**

WHEREAS, Business Associate and the Agency agree to also address herein the applicable requirements of the Security Rule, codified at 45 Code of Federal Regulations ("C.F.R.") Part 164, Subparts A and C, issued pursuant to the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA-AS"), so that the Covered Entity may meet compliance obligations under HIPAA-AS, the parties agree:

(a) **Security of Electronic Protected Health Information**. Business Associate will develop, implement, maintain, and use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information (as defined in 45 C.F.R. § 160.103) that Business Associate creates, receives, maintains, or transmits on behalf of the Plans consistent with the Security Rule.

(b) **Reporting Security Incidents within five (5) Business Days of Discovery**. Business Associate will report to the Plans any security incident of which Business Associate becomes aware that is (1) a successful unauthorized access, use or disclosure of the Plans' Electronic Protected Health Information; or (2) a successful major (a)

modification or destruction of the Plans' Electronic Protected Health Information or (b) interference with system operations in an information system containing the Plans' Electronic Protected Health Information. Upon the Plans' request, Business Associate will report any incident of which Business Associate becomes aware that is a successful minor (a) modification or destruction of the Plans' Electronic Protected Health Information or (b) interference with system operations in an information system containing the Plans' Electronic Protected Health Information.

(c) **Compliance Date**. The Business Associate certifies compliance with Section 8.0 on or before the date on which its representative signs this Agreement as set forth in the signature blocks below.

## Part III - HITECH REPORTING REQUIREMENTS

### 9.0 HITECH

In the event of any inconsistency or conflict between Part II and Part III, the more stringent provision shall apply.

Applicability of HITECH and HIPAA Privacy Rule and Security Rule Provisions. Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA), also known as the Health Information Technology Economic and Clinical Health (HITECH) Act, requires a Business Associate that contracts with the Agency, a HIPAA covered entity, to comply with the provisions of the HIPAA Privacy and Security Rules (45 C.F.R. 160 and 164).

(a). Reporting. The Business Associate shall make a good faith effort to identify any use or disclosure of protected health information not provided for in this Contract.

(b) To Covered Entity. The Business Associate will report to the Covered Entity, within ten (10) business days of discovery, any use or disclosure of protected health information not provided for in this Contract of which the Business Associate is aware. The Business Associate will report to the Covered Entity, within two (2) business days of discovery, any security incident of which the Business Associate is aware. The day the breach is discovered will be considered the first business day of the incident reporting period. A violation of this paragraph shall be a material violation of this Contract. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such breach.

(c) To Individuals. In the case of a breach of protected health information, as defined by HIPAA and HITECH, by the Business Associate, the Business Associate shall first notify the Covered Entity of the pertinent details of the breach and upon prior approval of the Covered Entity shall notify each individual whose unsecured protected health information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired or disclosed as a result of such breach. Such notification shall be in writing by first-class mail to the individual or personal representative (or the next of kin if the individual is deceased) at the last known address of the individual or next of kin or personal representative, respectively, or, if specified as a preference by the individual, by electronic mail. Where there is insufficient, or out-of-date contract information (including a phone number, email address, or any other form of appropriate communication) that precludes written (or, if specifically requested, electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting on the Web site of the covered entity involved or notice in major print of broadcast media, including major media in the geographic areas where the individuals affected by the breach likely reside. In any case deemed by the Business Associate to require urgency because of possible imminent misuse of unsecured protected health information, the Business Associate may also provide information to individuals by telephone or other means, as appropriate.

(d) To Media. In the case of a breach of protected health information discovered by the Business Associate where the unsecured protected health information of more than 500 persons is reasonably believed to have been,

accessed, acquired, or disclosed, after prior approval by the Covered Entity, the Business Associate shall provide notice to prominent media outlets serving the State or relevant portion of the State involved.

(e) To Secretary of Health and Human Services. The Business Associate shall cooperate with the Covered Entity to provide notice to the Secretary of Health and Human Services of unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals, such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the Business Associate may maintain a log of such breach occurring and annually submit such log to the Covered Entity so that it may satisfy its obligation to notify the Secretary of Health and Human Services documenting such breaches occurring in the year involved.

(f) Content of Notices. All notices required under this Attachment shall include the content set forth in the regulations implementing Section 13402(f), Title XIII of the American Recovery and Reinvestment Act of 2009, except that references therein to a "covered entity" shall be read as references to the Business Associate.

(g) Financial Responsibility. The Business Associate shall be responsible for reasonable costs related to the notices required under this Attachment.

(h) Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of protected health information in violation of this Attachment.

**Part IV**

**9.0 Miscellaneous**

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

(b) *Amendment.* Upon the enactment of any law or regulation affecting the use or disclosure of Protected Health Information, Standard Transactions, the security of Health Information, or other aspects of HIPAA-AS or the HITECH Act applicable or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either party may, by written notice to the other party, amend this Agreement in such manner as such party determines necessary to comply with such law or regulation. If the other party disagrees with such Amendment, it shall so notify the first party in writing within thirty (30) days of the notice. If the parties are unable to agree on an Amendment within thirty (30) days thereafter, then either of the parties may terminate the Agreement on thirty (30) days written notice to the other party.

(c) *Survival.* The respective rights and obligations of Business Associate under Section 7.0 of this Agreement shall survive the termination of this Agreement.

(d) *Interpretation.* Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule and the confidentiality requirements of the State of Florida, including section 110.123 (9), Florida Statutes.

(e) *No third party beneficiary.* Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assignees of the parties, any rights, remedies, obligations, or liabilities whatsoever.

(f) *Governing Law.* This Agreement shall be governed by and construed in accordance with the laws of the state of Florida to the extent not preempted by the Privacy Rules or other applicable federal law.

(g) The laws of the State of Florida shall apply to the interpretation of this Agreement or in case of any disagreement between the parties; the venue of any proceedings shall be the appropriate federal or state court in Leon County,

Florida.

(h) *Indemnification and performance guarantees.* Business Associate shall indemnify, defend, and save harmless the State of Florida and Individuals covered by the Plans for any financial loss as a result of the claims brought by third parties and which are caused by the failure of Business Associate, its officers, directors or agents to comply with the terms of this Agreement.

(i) *Independent Contractors*. Business Associate and Covered Entity are independent contractors and this Agreement will not establish any relationship of partnership, joint venture, employment, franchise, or agency between Business Associate and Covered Entity. Neither Business Associate nor Covered Entity will have the power to bind the other or incur obligations on the other party's behalf without the other party's prior written consent, except as otherwise expressly provided in this Agreement.

(j) *Conflicts.* In the event that any terms of this agreement are inconsistent with the terms of the Underlying Agreement, then the terms of this Agreement shall control.

Business Associate shall not assign either its obligations or benefits under this Agreement without the expressed written consent of the Covered Entity, which shall be at the sole discretion of the Covered Entity. Given the nature of this Agreement, neither subcontracting nor assignment by the Business Associate is anticipated and the use of those terms herein does not indicate permission to assign or subcontract has been granted.

| For the Agency: | For the Business Associate: |
|---|---|
| Department of Management Services | [Company Name Inc.] |
| By: _____ | By: _____ |
| C. Darren Brooks, Deputy Secretary | |
| Date: _____ | _____ |
| | (Print Name and Title) |
| | Date: _____ |