

EXHIBIT C

**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 C.F.R Part 164, Subparts A and C. (the “Security Rule”), the Health Information Technology For Economic and Clinical Health Act, enacted in Pub. L. No. 111-05 H.R., 111th Cong. (2009), Title XIII (the “HITECH Act”), as well as the confidentiality requirements contained in section 110.123 (9), Florida Statutes.

The Parties: The Florida Department of Management Services, Division of State Group Insurance (the “Covered Entity”).

_____, a _____ corporation, with its principal place of business at _____ (the “Business Associate”).

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 and 164.501, and in the HITECH Act, Subtitle D.

“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).

“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 at 45 CFR 160.103 and in the HITECH Act. For purposes of this Agreement, the term refers only to that Protected Health Information received directly or indirectly from, or received or created on behalf of, the Covered Entity.

“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 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.

2.0 Obligations and Activities of Business Associate Regarding Protected Health Information

- (a) Business Associate agrees to 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 of Florida.
- (b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

- (c) Business Associate agrees to 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) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
- (e) Business Associate agrees to 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) Business Associate agrees to 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) Business Associate agrees to 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.
- (h) Business Associate agrees to 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 Covered Entity, or at the request of the Covered Entity, 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) Business Associate agrees to 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) Business Associate agrees to provide to Covered Entity or an Individual 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.
- (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, will comply with the EDI Standards and the Annual Guidance.
- (l) Business Associate agrees to determine the Minimum Necessary type and amount of Protected Health Information required to perform its services and will comply with 45 CFR 164.502(b) and 514(d).

3.0 Permitted or Required Uses and Disclosures by Business Associate

- (a) Except as expressly permitted in writing by the Covered Entity, 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 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 Protected Health Information as necessary to provide the services required under the following service contract(s) with the Covered Entity: [Insert Name and Date of Contract].

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 Agreement Under State Law

- (a) Generally. 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 Covered Entity's 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 the Covered Entity, 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 the Covered Entity's 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:

- i. Appear at a deposition to give sworn testimony, and may also require that certain records be brought to be examined as evidence.
 - ii. 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.
 - iii. 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. Business Associate assumes responsibility and liability for any damages or claims, including state and federal administrative proceedings and sanctions, against the Covered Entity, 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.

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, of the laws of the State of Florida, if done by Covered Entity.

7.0 Term and Termination

- (a) Term. The Term of this Agreement shall begin on the last date set forth on the signature blocks below and shall terminate on the date the Business Associate no longer provides services to the Covered Entity.
- (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) Return or Destruction of PHI upon 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 intends to return or destroy such Protected Health Information. 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.

Prior to destroying any records hereunder, the Business Associate shall obtain written confirmation from the Covered Entity that such actions will not violate the State of Florida's record retention policies.

8.0 HIPAA Security Rule Addendum

- (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 Covered Entity consistent with the Security Rule.

- (b) Reporting Security Incidents. Business Associate will report to the Covered Entity any Security Incident of which Business Associate becomes aware that is (1) a successful unauthorized access, use or disclosure of any Electronic Protected Health Information; or (2) a successful major (a) modification or destruction of any Electronic Protected Health Information or (b) interference with system operations in an information system containing any Electronic Protected Health Information. Upon the Covered Entity's request, Business Associate will report any incident of which Business Associate becomes aware that is a successful minor (a) modification or destruction of any Electronic Protected Health Information or (b) interference with system operations in an information system containing any Electronic Protected Health Information.
- (c) Compliance Date. The parties to this Amendment will comply with Sections (a) through (c) of this Section 8 by the later of the (1) the last date set forth in the signature blocks below or (2) the compliance deadline of the Security Rule as defined in 45 C.F.R. § 160.103.

9.0 HITECH Act Compliance Agreement

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

- (a) Reporting. The Business Associate shall make a good faith effort to identify and report 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 twenty-four (24) hours of discovery, any Security Incident of which the Business Associate is aware. 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 discovered 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 the next of kin if the individual is deceased) at the last known address of the individual or next of kin, 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 Section 13402(f), Title XIII of the American Recovery and Reinvestment Act of 2009.
- (g) Financial Responsibility. The Business Associate shall be responsible for all 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.

10.0 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. All provisions in this Agreement that expressly or customarily survive the termination or expiration of the Agreement shall continue in effect after the Agreement is terminated or expires.
- (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. In the event of a dispute, venue of any proceedings shall be the appropriate federal or state court in Leon County, Florida.
- (g) Indemnification and Performance Guarantees. Business Associate shall indemnify, defend, and save harmless the State of Florida and Individuals for any financial loss as a result of 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.
- (h) Assignment. 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 that permission to assign or subcontract has been granted.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the Parties have executed this combined HIPAA Privacy Business Associate Agreement, Confidentiality Agreement, HIPAA Security Rule Addendum and HITECH Act Compliance Agreement, on the date(s) set forth below.

For: **Florida Department of Management Services**

For: **[Insert Name of Company]**

By: _____
Michelle Robleto, Director
Division of State Group Insurance

By: _____
Signature

Date: _____

(Print Name and Title)

Date: _____

Approved as to form and legality:

Office of DMS General Counsel

Date: _____