

**NON-CONTRACTUAL AGENCY AGREEMENT (NCA)  
(SOLE PROPRIETOR)**

This Agreement is between Florida Blue, on behalf of itself and its subsidiaries, Health Options, Inc. and Florida Combined Life (collectively "Company"), \_\_\_\_\_ ("Agency") a [corporation/limited liability company/partnership] organized under the laws of \_\_\_\_\_ and having its principal place of business at \_\_\_\_\_. Agency has read and fully understands the terms and conditions of this Agreement (the "Agreement"), and its attachments.

In signing this Agreement, Agency certifies that neither Agency nor any of its officers, directors, employees or sub-agents has been convicted of any criminal felony involving dishonesty or breach of trust or been convicted of an offense under Section 1033 of the Violent Crime Control and Law Enforcement Act of 1994. Agency further agrees to immediately inform the Company of any conviction of the types described in the preceding sentence.

To signify their agreement to the provisions of this Agreement, Company and Agency have made and entered into this Agreement as of \_\_\_\_\_ ("Effective Date").

**Florida Blue**

Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Agency:**

Signature : \_\_\_\_\_

Print Name: \_\_\_\_\_

EIN# \_\_\_\_\_

Title : \_\_\_\_\_

Date : \_\_\_\_\_

**Florida Combined Life, Inc.**

Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Email: \_\_\_\_\_

**Health Options, Inc.**

Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Once completed, please return this page to Florida Blue**

FLORIDA BLUE DOES NOT DISCRIMINATE ON THE BASIS OF RACE, COLOR, NATIONAL ORIGIN, DISABILITY, AGE, SEX, GENDER IDENTITY, SEXUAL ORIENTATION, OR HEALTH STATUS IN THE ADMINISTRATION OF THE PLAN, INCLUDING ENROLLMENT AND BENEFIT DETERMINATIONS.

## AGENCY AGREEMENT (SOLE PROPRIETOR)

This Agreement is between Florida Blue, on behalf of itself and its subsidiaries, Health Options, Inc. and Florida Combined Life (collectively "Company"), \_\_\_\_\_ ("Agency") a [corporation/limited liability company/partnership] organized under the laws of \_\_\_\_\_ and having its principal place of business at \_\_\_\_\_. Agency has read and fully understands the terms and conditions of this Agreement (the "Agreement"), and its attachments.

In signing this Agreement, Agency certifies that neither Agency nor any of its officers, directors, employees or sub-agents has been convicted of any criminal felony involving dishonesty or breach of trust or been convicted of an offense under Section 1033 of the Violent Crime Control and Law Enforcement Act of 1994. Agency further agrees to immediately inform the Company of any conviction of the types described in the preceding sentence.

To signify their agreement to the provisions of this Agreement, Company and Agency have made and entered into this Agreement as of \_\_\_\_\_ ("Effective Date").

### Florida Blue

Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

### Agency:

Signature : \_\_\_\_\_

Print Name: \_\_\_\_\_

EIN# \_\_\_\_\_

Title : \_\_\_\_\_

Date : \_\_\_\_\_

### Florida Combined Life, Inc.

Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Email: \_\_\_\_\_

### Health Options, Inc.

Signature: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**Please retain the rest of the contract (including this page) for your records**

FLORIDA BLUE DOES NOT DISCRIMINATE ON THE BASIS OF RACE, COLOR, NATIONAL ORIGIN, DISABILITY, AGE, SEX, GENDER IDENTITY, SEXUAL ORIENTATION, OR HEALTH STATUS IN THE ADMINISTRATION OF THE PLAN, INCLUDING ENROLLMENT AND BENEFIT DETERMINATIONS.

**AGENCY AGREEMENT  
(SOLE PROPRIETOR)**

**A. Duties and Authority of Agency**

- 1) a) Agency shall solicit from groups and members of the general public, applications for the products included in Addendum "A" ("Company Products"), which is hereby made a part of this Agreement. Agency is only authorized to solicit business for, and this Agreement only applies to, the products included in Addendum "A". Agency shall solicit for Company Products only though those individuals listed on a Designated Producer Addendum.
  - b) Agency shall notify Company of any proposed changes to the list of Designated Producers on the Designated Producer Addendum no later than ten (10) calendar days after the end of the calendar month in which such change is proposed to be effective. No such proposed change shall be effective until accepted by Company. Also, where such proposed change involves Agency adding a new Designated Producer, such change shall not be effective until (i) Company has determined, in its reasonable discretion, that the proposed Designated Producer is appropriately qualified, and (ii) the proposed Designated Producer, Agency and Company execute a Designated Producer Addendum.
  - c) Agency's authority under this Agreement is non-exclusive.
  - d) The Company shall appoint Agency's Designated Producers to represent Company to perform the obligations described in this Agreement relative to the products identified in Addendum "A." During the Appointment of Agency's Designated Producers, Agency shall carry out said obligations in the manner described in this Agreement and as otherwise communicated to Agency by Company. In order to maintain the Appointments for Agency's Designated Producers, Agency shall abide by the requirements of Addendum "B," which is hereby made a part of this Agreement.
- e) Agency shall be solely responsible for the supervision of all Designated Producers and shall ensure that all Designated Producers comply with applicable law, the terms of this Agreement and the applicable Designated Producer Addendum. The Agency's use of Designated Producers shall not relieve Agency of any liability to Company for the proper and lawful performance of Agency's duties under this Agreement.
- 2) Agency will service Company group accounts and insureds issued Company Products as a result of applications submitted by Agency (hereinafter, referred to as "Insured" or "Insureds"). Such service will include, but not be limited to, the following:
    - a) Soliciting, through Designated Producers, applications and related documents required by Company for Company Products prior to effectuating insurance coverage and forwarding those documents promptly to the Company for its consideration;
    - b) Receiving the initial premiums for Company Products and where received by a Designated Producer, collecting such premium from the Designated Producer. Agency shall submit the full amount received and collected promptly to the Company
    - c) Assisting a family member/dependent to obtain other appropriate coverage when he or she is no longer entitled to coverage by a Company Product as a family member, e.g., when a dependent child reaches the limiting age, or upon a divorce or a dissolution of marriage; and

- d) Maintaining a working and current knowledge of Company Products and the ability to explain the terms of coverage.
- 3) Agency, for itself and its Designated Producers, agrees to secure and maintain licenses and appointments by Company as is necessary to transact business on behalf of Company and as required by Florida law. Agency shall provide Company copies of all required licenses, including licenses for all Designated Producers. Agency further agrees to notify Company immediately of any expiration, termination, suspension or other action by the Office of Insurance Regulation or any other governmental agency affecting said licenses or appointments. Agency further agrees to notify Company in writing immediately upon receiving notice with respect to Agency or any Designated Producer of any misdemeanor or felony charges or any actions including, but not limited to, convictions by any governmental authority for commission of any act involving fraud, dishonesty, breach of trust, theft, misappropriation of money or breach of any fiduciary duty.
- 4) a) Agency agrees to comply with the rules of Company relating to the completion and submission of applications, actively participate in and facilitate enrollment meetings for Company Products, and to make no representation with respect to the terms of coverage of any Company Product not in conformity with the material prepared and furnished to Agency for that purpose by Company.
- b) Agency shall use best efforts to ensure that each application for a Company Product is fully and truthfully completed by the applicant and the completed application fully and accurately reflects and discloses the circumstances, including the health condition, of persons for whom a Company Product is sought in the application, as applicable. Agency further agrees to inform every applicant that Company will rely upon said representations in the underwriting process, and that the subsequent discovery of material facts known to applicant and either not disclosed or misrepresented may result in the rescission of any Company Product. Agency will also inform the applicant that in no event will the applicant have any coverage unless and until the application is reviewed and approved by the Company and a policy is issued.
- 5) Agency is not authorized to, and agrees not to, enter into, alter, deliver or terminate any policy on behalf of Company, extend the time of payment of any charges or premiums, or bind Company in any way without the prior written permission of Company. Agency acknowledges and agrees that Company reserves the right, in accordance with applicable law, to reject any and all applications submitted by Agency.
- 6) Agency is not authorized to receive any Company funds except the initial premiums for Company Products, and Agency is not authorized to deduct compensation, commissions, service fees or allowances from any initial premiums Agency may collect. Any funds that Agency does receive for or on behalf of Company, either directly or through Designated Producers, shall be received and held by Agency in a fiduciary capacity, shall be separately accounted for, shall not be commingled by Agency with personal funds of Agency or other business accounts managed or owned by Agency, and shall be remitted to Company promptly but in no event later than five (5) calendar days from the date of receipt.
- 7) Agency shall not broadcast, publish or distribute any advertisements or other material relating to Company Products, not originated by Company, nor use the name, trademark or logo of Company or any of its subsidiaries or affiliates in any way or manner without Company's prior written consent and then only as specifically authorized in writing by Company. The restrictions on promotional and descriptive material included in this Paragraph 7 includes, but is not limited to, internet communications or any other electronic transmissions representing Company Products, brochures, telephone directory advertisements (print or electronic) and Agency company

listings.

- 8) Agency agrees to maintain for Agency and all Designated Producers complete and separate records for Company for a period of at least seven (7) years of all transactions pertaining to applications submitted to Company, and any other documents as may be required by the Florida Office of Insurance Regulation or other governmental agency. Any and all records described above or as may otherwise relate to Agency's activities in connection with Company business shall be accessible and available to representatives of Company and Company's regulators who may audit them from time to time while this Agreement is in effect or within seven (7) years after termination thereof.
- 9) Agency agrees to obtain and maintain Errors and Omissions Insurance coverage with minimum amounts of \$500,000 per occurrence and \$1,000,000 in aggregate or such higher amounts as may be required by law or as determined by Company and from a carrier satisfactory to Company. Agency shall ensure that all Designated Producers obtain and maintain such coverage. Agency shall provide to Company upon request certificates of insurance evidencing such coverage for Agency and Designated Producers. Agency agrees to make best efforts to provide Company with thirty (30) days prior written notice, and in any event will provide notice as soon as reasonably practicable, of any modification, termination or cancellation of such coverage.
- 10) Agency is an independent contractor and shall have no claim to compensation except as provided in this Agreement and Agency shall not be entitled to reimbursement from Company for any expenses incurred in performing this Agreement. Agency further agrees that to the extent of any indebtedness to Company from Agency, Company shall have a first lien against any commissions due Agency, and such indebtedness may be deducted at the Company's option from any commissions due Agency. Moreover, this Agreement does not give Agency any power of authority other than as expressly granted herein and no other or greater power shall be implied from the grant or denial of powers specifically mentioned herein.
- 11) Agency will treat as trade secrets any and all information concerning customers of Company or its business, products, techniques, methods, systems, price-books, rating tools, plans or policies; and Agency will not, during the term of this Agreement or at any time thereafter, disclose such information, in whole or in part, to any person, firm or corporation for any reason or purpose whatsoever, or use such information in any way or in any capacity other than as a sales agent of Company in furtherance of Company's interests. Upon termination of this Agreement, or sooner if requested by any Company, Agency will immediately deliver to Company any and all literature, documents, data, information, order forms, memoranda, correspondence, customer and prospective customer lists, customer orders, records, cards or notes acquired, compiled or coming into Agency's knowledge, possession, custody or control in connection with his/her activities as a sales agent or sales representative of Company, as well as all machines, parts, equipment, rating tools and other materials received by Agency from Company or from any of its customers, agents or suppliers in connection with such activities. Upon termination of any Designated Producer Addendum or upon the termination of this Agreement, Agency will, at the request of the Company, collect from the Designated Producer(s) any of the documents, information or other items specified in the immediately preceding sentence from the applicable Designated Producer(s).
- 12) Agency shall cooperate fully with Company in any investigation or proceeding of any regulatory or governmental body, or court of competent jurisdiction, including, where required by law, making its books and records available to such entities for inspection, if it is determined by Company that the investigation or proceeding affects matters covered by, related to, or arising out of this Agreement.
- 13) Agency shall defend any act or alleged act of Agency, including, without limitation, any act or alleged act of Designated Producers, at Agency's own expense. Agency shall reimburse Company for all costs, expenses or

legal fees that Company incurs for the defense of any administrative action in which Company or Agency or any Designated Producer is named and which is determined by a court of competent jurisdiction or by an appointed arbitrator to be the consequence of any unauthorized act of Agency or a Designated Producer.

- 14) During and after the term of this Agreement, Agency shall indemnify, defend and hold Company harmless from and against any loss, damage or expense, including reasonable attorneys' fees, caused by or arising from the negligence, misconduct or breach of this Agreement by Agency or any Designated Producer, or from the failure of Agency or any Designated Producer to comply with any federal or state laws, rules or regulations, and excluding any negligent acts, omissions or willful misconduct by Company, its Directors, Officers, Agents or Employees.

- 15) In the event Company determines that Agency has failed to (1) perform its responsibilities and duties in a reasonable and professional manner, or as required by this Agreement or as otherwise communicated by Company; or (2) act in a manner consistent with Company's policies and procedures, Company reserves the right to place Agency's Designated Producers Appointments in a probationary status during which time Company may enforce corrective action against Agency including, for example, refusing to accept new business from Agency.

#### B. Commission Rules

- 1) For Company Products produced by Agency and Designated Producers (and as applicable, for any other Company policies or contracts Agency was authorized to sell and produced in the past-see Appendix 1 to Addendum A for a complete list of such policies), Company will pay to Agency commissions and renewal fees in accordance with the rates and schedules outlined in Addendum "C," which is hereby made part of this agreement, provided that Agency is in compliance with all items listed in said Agreement.
- 2) As indicated above, all commissions or other compensation payable with respect to Company Products produced by Designated Producers acting for the Agency shall be paid by Company to Agency and not to Designated Producer. The Company's payment of all such commissions or other compensation to Agency shall be subject to all the terms and conditions of this Agreement. Agency shall separately agree with each Designated Producers regarding a basis for Agency to compensate Designated Producer for its activities under the applicable Designated Producer Addendum. Designated Producer shall have no claim or right whatsoever against Company for any commissions or other compensation, and Agency shall take no action to indicate otherwise.
- 3) Notwithstanding anything stated in this Agreement to the contrary, Agency shall not receive any commission or compensation (including, without limitation, commissions for renewals or additional coverage or enrollments) with respect to any Company Products or other Company policies or contracts produced by an individual for the Company prior to or after the period during which such individual is a Designated Producer for Agency.
- 4) Agency shall pay over promptly (within 5 business days) to the Company gross payments and other monies received or collected on behalf of the Company and shall not deduct or subtract or retain therefrom commissions or any other fees which may be payable hereunder.
- 5) Commissions will only be paid when both of the following criteria are satisfied:
- a) Premiums received and retained by the Company.
  - b) Applications submitted by Agency and accepted by Company.
- 6) Commissions become payable only after the due date of the premium payment and the gross payment due has been received in full and has been processed by the Company.
- 7) In the event that insured terminates coverage with Company within the first twelve (12) months of plan, Company will deduct prorated amount from any sums due or becoming due to Agency by Company.

- 8) No commissions will be payable on account of waived payments or payments refunded for any reason. Any commissions received on account of any waived or refunded payments shall be deducted from future commission payments, if available, or shall be returned in full to the Company, within 5 business days of notification, by the Agency and shall constitute indebtedness to the Company until returned.
- 9) Company reserves the right to periodically make changes to the following:
  - a) Company reserves the right to change Company's commission schedules (including renewal fees) at any time after providing sixty (60) days prior written notice of the commission and renewal fee change to Agency.
  - b) Company shall have the right to develop and implement incentive programs related to Agency's sales activities.
  - c) In the event Agency wishes to contest a payment (i.e., a payment involving a specific claim or case, as opposed to an alleged "programmatic payment error") made under this Section, notice shall be given to Company within 365 calendar days from the date of the disputed payment. Any such payment request exceeding the 365 calendar day period will not be considered by Company.
- 10) Agency may assign commissions payable with respect to policies produced by that Agency and issued by the Company to another licensed agent provided all of the following conditions are satisfied:
  - a) Agency must have prior approval from the Company.
  - b) The assignment must be in writing and in a form acceptable to the Company, in its sole discretion.
  - c) Under the terms of the assignment, the agent to whom the commissions are assigned must expressly agree to abide by the terms of this Agreement and assume all of the Agency's obligations and responsibilities to the Company and the Insureds under this Agreement with

respect to the policies for which commissions are being assigned.

- d) Any purported assignment or transfer of any interest in Agency's commissions other than in strict compliance with the terms stated in this Agreement shall be void to the Company.

#### C. Term and Termination

- 1) This Agreement shall be effective for an initial term of one (1) year from the Effective Date, and thereafter shall automatically renew for additional terms of one (1) year each, unless and until terminated in accordance with the provisions of this Agreement.
- 2) This Agreement may be terminated without cause at any time by Agency or Company by either party giving thirty (30) days prior written notice thereof to the other party.
- 3) Company may terminate this Agreement immediately upon written notice to Agency at any time upon material default or substantive breach by Agency of one or more of its obligations under this Agreement (including any amendments), or Agency's commission of fraud, dishonesty, breach of trust, theft, misappropriation of money, or breach of any fiduciary duty. Agency's failure to comply with any provision of this Agreement shall be material if Company determines that such failure affects Agency's ability to perform under this Agreement. Termination for cause shall not be Company's exclusive remedy, but shall be cumulative with all other remedies available at law or in equity. A failure to terminate this Agreement for cause shall not be a waiver of the right to do so with respect to any past, current or future default.
- 4) This Agreement will automatically terminate in the event the Agency files a petition for bankruptcy or becomes insolvent or upon attachment of the Agency's business, records or accounts pursuant to any order of a court.
- 5) This Agreement will automatically terminate upon the death of all Designated Producers of Agency.
- 6) Commission Settlement On Termination

Commission payments will immediately cease (and no further commissions will become payable after the termination date) in the event of the following:

- i) Dissolution/Termination of the Agreement - to include with and without cause agreement terminations.
- ii) Agent of Record Change in such an event when Agency is no longer designated as the "Agent of Record" by an insureds, Company shall appoint a new Agent of Record to the insureds.
- iii) Agency induces or attempts to induce insureds to surrender or terminate policies with Company.
- iv) Agency is no longer servicing insureds in a manner that is satisfactory to the Company.
- v) Ninety (90) days after (X) Agency is no longer licensed as an insurance agent in the state of Florida (if such licensing is required), (Y) none of Agency's Designated Producers remain licensed as an insurance agent in the state of Florida or (Z) none of Agency's Designated Producers remain appointed with Company, unless commissions during this ninety (90) day period are not permitted by applicable law.

#### D. Settlement of Disputes

Except for equitable relief for breaches of Section E, if any disagreement between the Agency and the Company should arise between the Agency and the Company related to the interpretation or performance of this Agreement, including its formation or validity, or any transaction under this Agreement whether arising before or after its termination, the Agency and the Company shall make a good faith effort to settle such disagreement. However, if they are unable to settle such disagreement within thirty (30) days, or such longer period as may be agreed upon by both parties, then such disagreement

shall be submitted to arbitration at the request of either party for settlement in accordance with the rules of the American Arbitration Association for commercial disputes, except as may be modified below. The following procedure shall apply:

- a) The party requesting arbitration shall so notify the other party in writing and shall specify the points of disagreement to be arbitrated.
- b) Within fifteen (15) days after receipt of such notification, the Agency and the Company shall each select an arbitrator and give his or her name and address to the other. These two arbitrators shall promptly select a third arbitrator, who shall be the umpire. All arbitrators selected shall be disinterested, former or active executives of a life and health insurance company or agency. If a party fails to appoint its arbitrator within the fifteen (15)-day time limit, the other party shall appoint the second arbitrator. If the two arbitrators fail to agree upon the appointment of an umpire within fifteen (15) days after their appointment, each of them shall, on the sixteenth (16th) day, name three nominees, of whom the other shall decline two and the selection of the umpire from the remaining two nominees shall be made by drawing lots.
- c) The arbitrators shall make all decisions consistent with the customs and practices of the insurance business, and with a view to effect the general purpose of the Agreement in a reasonable manner. The arbitrators shall be prohibited from awarding punitive, exemplary, treble or consequential damages of whatever nature.
- d) The written and signed decision of a majority of the three arbitrators, consistent with the provisions of part c. above, shall be final and binding on the Agency and the Company. A copy of the decision shall be given to each the Agency and the Company within sixty (60) days after the date of the request for arbitration.
- e) All expenses of arbitration shall be borne equally by the Agency and the Company.

E. Privacy and Security

1) Privacy and Security of Protected Health Information.

For this Section E, “Agency” shall be referenced as “Business Associate.”

- a) Permitted Uses and Disclosures. Except as otherwise limited in Section E, Business Associate may use this disclose or request the minimum necessary Protected Health Information and Nonpublic Personal Financial Information to perform functions, activities, or services for, or on behalf of, Company as specified in this Agreement, provided that such use, disclosure or request would not violate the HIPAA-AS Privacy Rule if done by Company.
- b) Prohibition on Unauthorized Use or Disclosure. Business Associate shall not use or disclose Protected Health Information or Nonpublic Personal Financial Information other than as permitted or required by Section E or as required by Law.
- c) Information Safeguards and Breach Reporting.
  - (i) Privacy of Protected Health Information. Business Associate shall use appropriate safeguards to prevent use or disclosure of Protected Health Information and Nonpublic Personal Financial Information not provided for by this Section E.

Business Associate shall report in writing to Company’s Corporate Compliance Office any use or disclosure of Protected Health Information or Nonpublic Personal Financial Information not provided for by this Section E as soon as practicable but no later than five (5) days after Business Associate becomes aware of such unauthorized use or disclosure. Unless otherwise directed by Company’s Corporate

Compliance Office, Business Associate shall include in the report the following:

- (A) the date of the unauthorized use or disclosure;
  - (B) the name and (if known) address of the person or entity which received Protected Health Information pursuant to the unauthorized disclosure;
  - (C) a brief description of the Protected Health Information that was the subject of the unauthorized use or disclosure;
  - (D) a brief statement of the nature of the unauthorized use or disclosure;
  - (E) the name and date of birth of the individual(s) whose Protected Health Information was the subject of the unauthorized use or disclosure, and each such individual’s contract number;
  - (F) the corrective action that Business Associate has taken or will take to prevent further unauthorized uses or disclosures; and
  - (G) the steps Business Associate has taken or will take to mitigate any known harmful effects of the unauthorized use or disclosure.
- (ii) Security of Electronic Protected Health Information. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information.

Business Associate shall report in writing to Company’s Corporate Compliance Office any successful Security Incident as soon as practicable but no later than five (5) days after Business Associate becomes aware of such Security Incident and shall submit

- follow-up documentation pursuant to the direction of Company's Corporate Compliance Office. Upon Company's request and pursuant to Company's direction, Business Associate shall report in writing any attempted but unsuccessful Security Incident of which Business Associate becomes aware. Business Associate shall comply with this Section E (1) (C).
- d) Mitigation. Business Associate shall mitigate to the extent practicable any harmful effect of which Business Associate is aware that is caused by any use or disclosure of Protected Health Information or Nonpublic Personal Financial Information not provided for by Section E.
  - e) Agents and Subcontractors. Business Associate shall ensure that its agents and subcontractors to whom it provides Protected Health Information agree in writing to the same privacy and security restrictions and conditions that apply through Section E to Business Associate with respect to such information.
  - f) Business Associate Guidance. Business Associate shall comply with any policy, procedure or guidance with respect to Business Associate's responsibilities under Section E that Company may, from time to time, issue and communicate in writing to Business Associate.
- 2) Management of Protected Health Information.
- a) Access. Business Associate shall, within seven (7) days following Company's request, make available to Company for inspection and copying Protected Health Information about an individual that is in Business Associate's custody or control, so that Company may meet its access obligations under the HIPAA-AS Privacy Rule.
  - b) Amendment. Business Associate shall, within fourteen (14) days following Company's request, amend or permit Company to amend any portion of Protected Health Information that is in Business Associate's custody or control so that Company may meet its amendment obligations under the HIPAA-AS Privacy Rule.
  - c) Disclosure Accounting. Business Associate shall record the information specified below ("disclosure information") for each disclosure of Protected Health Information that Business Associate makes, excluding disclosures identified in 45 CFR § 164.528(a)(1) including but not limited to disclosures for Treatment, Payment, and Health Care Operations and disclosures pursuant to a HIPAA-AS compliant authorization, and shall report the disclosure information to Company's Corporate Compliance Office at P.O. Box 44283, Jacksonville, Florida 32203-4283 in writing within five (5) days of Business Associate making the accountable disclosure. Disclosure information shall include:
    - (i) the disclosure date;
    - (ii) the name and (if known) address of the person or entity to which Business Associate made the disclosure;
    - (iii) a brief description of the Protected Health Information disclosed;
    - (iv) a brief statement of the purpose of the disclosure;
    - (v) the name and date of birth of the individual whose Protected Health Information was disclosed; and
    - (vi) that individual's contract number.
  - d) Inspection of Internal Practices, Books and Records. Business Associate shall make its internal practices, books, and records relating to its use and disclosure of Protected Health Information and its protection of the confidentiality, integrity, and availability of Electronic Protected Health Information available to Company

and the U.S. Department of Health and Human Services (“HHS”) as requested or required to determine Company’s compliance with the

#### HIPAA-AS Privacy Rule and Security Rule Breach of Privacy and Security Obligations

##### a) Termination of Addendum.

- (i) Company and Business Associate specifically acknowledge and agree that a breach of any term of this Section E shall be considered a breach of a material term of the Agreement and Company may terminate the Agreement in accordance with the Agreement’s termination provision.

##### b) Obligations on Termination.

- (i) Return or Destruction of Protected Health Information. Upon termination of the Agreement, Business Associate shall, if feasible, return to Company or destroy all Protected Health Information in its custody or control in whatever form or medium, including all copies and all derivative data, compilations, and other works that allow identification of an individual who is a subject of the Protected Health Information. Business Associate shall in writing identify to Company any Protected Health Information that cannot feasibly be returned to Company or destroyed and explain why return or destruction is infeasible. Business Associate shall limit further use or disclosure of such Protected Health Information to those purposes that make its return or destruction infeasible. Business Associate shall complete these obligations as promptly as possible, but not later than thirty (30) days following the effective date of the termination of the Agreement.
- (ii) Continuing Privacy and Security

Obligations. Business Associate’s obligation to protect the privacy and confidentiality and safeguard the security of Protected Health Information specified in Section E shall be continuous and survive termination of the Agreement

##### 4) General Provisions for this Section E.

- a) Definitions. The terms “Electronic Protected Health Information” and “Protected Health Information” have the meanings set out in 45 CFR § 160.103, except Protected Health Information shall be limited to that information created or received by Business Associate from or on behalf of Company pursuant to the Agreement. The term “Required by Law” has the meaning set out in 45 CFR § 164.103. The term “Security Incident” has the meaning set out in 45 CFR § 164.304. The terms “Health Care Operations,” “Payment,” and “Treatment” have the meanings set out in 45 CFR § 164.501. For purposes of this Addendum, Protected Health Information encompasses Company’s Electronic Protected Health Information. The term “Nonpublic Personal Financial Information” has the meaning set out in Fla. Admin. Code § 4-128.002 except Nonpublic Personal Financial Information shall be limited to that information created or received by Business Associate from or on behalf of Company pursuant to this Agreement.
- b) Amendment to this Section E. This Section E shall automatically amend upon the compliance date of any final regulation or amendment to final regulation promulgated by HHS or a Florida regulatory agency concerning the subject matter of Section E such that Business Associate’s obligations remain in compliance with the final regulation or amendment to final regulation, unless Company or Business Associate elects to terminate Section E by giving the other party written notice of termination at least ninety (90) days before

the compliance date of such final regulation or amendment to final regulation.

- c) **No Third Party Beneficiaries.** No party shall be deemed a third party beneficiary of Section E.

**F. General Terms**

- 1) **Entire Agreement.** As of the Effective Date of this Agreement, this Agreement (including any attached addendums or schedules) is the complete and sole contract between the parties regarding the distribution and renewal of Company Products (and as applicable, any other Company policies or contracts) by Agency and supersedes any and all prior understandings or agreements between the parties whether oral or in writing on this subject matter. For the avoidance of doubt, this Agreement replaces all Single Case Agreements between the parties executed prior to the Effective Date, including, without limitation, with respect to commission or other compensation payable for Company Products (and as applicable, other Company policies or contracts) issued prior to or after the Effective Date.
- 2) **Construction.** In this Agreement the words "shall" and "will" are used in the mandatory sense. Unless the context otherwise clearly requires, any one gender includes all others, the singular includes the plural, and the plural includes the singular.
- 3) **No Waiver.** The fact that Company may not have insisted upon strict compliance with this Agreement with respect to an act or transaction of Agency shall not relieve Agency from the obligation to perform strictly in accordance with the terms of this Agreement.
- 4) **Independent Contractor.** Agency shall be an independent contractor of Company, and nothing herein shall be construed as creating a relationship of employer-employee, partner, joint venturer, officer or agent of Company in any manner for any other purpose, other than as specifically provided in this Agreement.
- 5) **Applicable Law.** This Agreement shall be governed by the laws of the State of Florida, without regard to its choice of law provisions.
- 6) **Limitation of Liability.** Company's liability, if any, for damages to Agency for any cause whatsoever arising out of or related to this Agreement, and regardless of the form of the action, shall be limited to Agency's actual damages. Company shall not be liable for any indirect, incidental, punitive, exemplary, special or consequential damages of any kind whatsoever sustained as a result of a breach of this Agreement or any action, inaction or alleged tortious conduct or delay by Company.
- 7) **Survival.** In addition to those provisions which by their terms survive expiration or termination of this Agreement, Paragraphs 8 and 10-14 of Section A; and Sections B, D, E and F shall survive expiration or termination of this Agreement, regardless of the cause giving rise thereto.
- 8) **No Third Party Beneficiaries.** Nothing express 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 permitted assigns of the parties, any rights, remedies, obligations or liabilities whatsoever.
- 9) **Amendment.** Except as stated in Section C, Company may modify this Agreement upon thirty (30) days prior written notice to Agency. Notwithstanding the foregoing, upon the enactment of any law or regulation, or any order or direction of any governmental agency affecting this Agreement (including, without limitation, Section C of this Agreement), Company may, by written notice to Agency, amend the Agreement in such manner as Company determines necessary to comply with such law or regulation, or any order or directive of any governmental agency. Company may provide written notice pursuant to this Paragraph 9 by letter, newsletter, electronic mail or other media.
- 10) **Relationship of Florida Blue Association -** This Agreement constitutes an agreement solely between Company and Agency and Company is an independent corporation operating under a license from the Florida Blue Association, an association of independent Florida Blue Plans

(the "Association") permitting Company to use the Florida Blue service marks in accordance with the Florida Blue Association's licensing standards and that Company is not contracting as the agent of the Association. Agency has not entered into this Agreement based upon representations by any persons other than Company and no person, entity, or organization other than Company shall be held accountable or liable to Agency for any of Company's obligations under this Agreement.

- 11) *Compliance with Law.* As applicable to this Agreement, Company and Agency shall comply with all laws and regulations applicable to their businesses, their licenses and the transactions into which they enter.
- 12) *Fiduciary Capacity.* Agency agrees that in performing under this Agreement Agency is acting in a fiduciary capacity to Company. Agency shall act in the best interest of Company. Agency shall not permit other interests, activities or responsibilities to interfere with Agency's faithful performance under this Agreement.
- 13) *Assignment.* Except as specifically provided in Paragraph 9 of Section B, neither this Agreement nor the right to receive money hereunder may be assigned without the prior written consent of Company, and any assignment made contrary to this provision shall be void as to Company; provided, however, Company may assign, delegate or transfer this Agreement in whole or in part to any affiliate, now or in the future, or to any entity which succeeds to the applicable portion of its business through a sale, merger or other transaction, provided to such other entity assumes the obligations of Company hereunder. This Agreement is personal to Agency, and Agency's duties hereunder shall not be delegated or subcontracted by Agency. Agency shall not use subagents.
- 14) *Notice.* Any notice required from Company under this Agreement shall be deemed given on the day such notice is deposited in the United States mail with first class postage pre-paid and addressed to Agency at the

address of the Agency appearing on the records of Company. Any notice required from Agency shall be deemed given on the date after such notice is deposited in the United States mail with first class postage pre-paid and addressed to Vice President, Corporate Sales, Florida Blue, 4800 Deerwood Campus Parkway, , Jacksonville, Florida, 32246.

- 15) *Force Majeure.* Any delay or failure of a party hereto to perform its obligations under this Agreement shall not be deemed to be a breach of this Agreement and shall otherwise be excused to the extent that, the delay or failure is caused by an event or occurrence beyond the reasonable control of the party and without its fault or negligence, including (but not limited to) acts of God, severe weather, wars, revolution, civil commotion, acts of public enemy or terrorism, embargo, action by any governmental or regulatory authority, natural disasters, sabotage, strikes, slowdowns, picketing or boycotts, power failures, nuclear hazard, or court injunction or order (a "Force Majeure Event"). Any party claiming that a Force Majeure Event has arisen shall (i) promptly notify the other party of the same, (ii) take all commercially reasonable steps to overcome and remove the effects of the Force Majeure Event, (iii) notify the other Party on a continuing basis of its efforts to overcome the Event of Force Majeure Event and (iv) promptly notify the other party when said condition has ceased.
- 16) *Electronic Notices, Waivers and Amendments.* Except as provided in Paragraph 9 of Section F, for purposes of providing notices required or permitted by this Agreement, waiving any right under this Agreement, or amending any term of this Agreement and notwithstanding any law recognizing electronic signatures or records, "a writing signed," "in writing" and words of similar meaning, shall mean only a writing in a tangible form bearing an actual "wet" signature in ink manually applied by the person authorized by the respective party, unless the parties agree otherwise by making a specific reference to this section.

# COMPENSATION ADDENDUM COMMISSIONS SCHEDULE JANUARY 1, 2025 - DECEMBER 31, 2025, CALENDAR YEAR

The original effective date of this Agreement is January 1, 2025. This Agreement will solely govern the amount of all Commissions and/or Renewal Fees payable to the Agency, including for Company Products (or as applicable, any other Company policies or contracts Agency was previously authorized to sell). Florida health insurance products are only for Florida residents with a physical address in Florida.

## FLORIDA BLUE AND HEALTH OPTIONS, INC. COMMISSION SCHEDULE

### Base Commission:

Small Group 4-50 Category Per Contract Per Month Rate [SimplyBlue, Truli for Health, BlueCare, BlueOptions, BlueSelect, and BlueChoice Products only]			
Location	BluePartners Classification	New Sales	Renewals
South Florida and Treasure Coast	BlueDiamond	\$40	\$36
	Blue Preferred	\$36	\$32
	Blue Standard Plus	\$32	\$28
	Blue Standard	\$32	\$28
Remaining Florida	BlueDiamond	\$34	\$30
	Blue Preferred	\$30	\$26
	Blue Standard Plus	\$26	\$22
	Blue Standard	\$26	\$22

Small Group 1-3 Category Per Contract Per Month Rate [SimplyBlue, Truli for Health, BlueCare, BlueOptions, BlueSelect, and BlueChoice Products only]			
Location	BluePartners Classification	New Sales	Renewals
All Florida	All Classifications	\$3	\$3

### Group Base Commission General Assumptions

- Commission rates are determined based on group category as of the group's new sale and renewal month.
- Group categories are determined at the renewal date. Any changes to the group category will not take effect until the next renewal date.
- The group category is determined by the number of eligible employees. Groups with 1-50 eligible are classified as Small Group. 51+ eligible are classified as Large Group.
- Compensation is determined based on a combination of group category and number of employees enrolled.
  - Small Groups with 1-3 enrolled contracts are included in the 1-3 category for compensation purposes.
  - Groups with 4-50 enrolled are included in the 4-50 category for compensation purposes.
- Rating category for non-grandfathered large groups is based on average number of employees.

- Contract count is based on month ending in-force contracts (including FHCP groups).
- Agents must obtain a separate appointment with BeHealthy Florida (hereby referred to as Truli for Health) to be eligible for Truli for Health compensation.
- Commissions paid in error or overpayments must be repaid to Florida Blue/HOI. If a group cancels, commissions are charged back based on the group cancellation date. For groups that reinstate, commissions are paid retroactive to the reinstatement date based on the contract count at the time of reinstatement.
- No adjustments are paid for any contracts that are added or terminated retroactively for active groups.

### **Small Group Base Commission Assumptions**

- South Florida is defined as Palm Beach, Broward, and Miami-Dade counties. Treasure Coast is defined as Indian River, Martin, and St. Lucie counties. Monroe County is not included in South Florida for commission purposes.
- Location-specific rates are based on county of group headquarters.
- All new and existing 1-50 category groups that become effective or renew with Florida Blue/HOI are paid based on the Per Contract Per Month (PCPM) basis.
- Renewal enrollment count is established 120 days prior to the anniversary date. In the event there is a change of 15% or more in the enrollment count at the time of actual renewal month, the group commission rate is based on the change.
- If an agency experiences a classification change during the year, the commission on existing groups will not change until the renewal of the group

### **Large Group Base Commission Assumptions**

- For group sizes 51+, Florida Blue/HOI pays commissions based on negotiated rates.
- Commissions calculated as a percentage of premiums are based upon reconciled premium only.
- For group sizes 51+, any change of commission rate requires the group to be re-rated with the new commission amount.
- Agencies working with a GA (Wholesaler) for group size 51+ are required to split commissions in accordance with negotiated rates

## Group Retiree Commissions

Group Retiree Product*	New Sale Rates	Renewal Rates
BlueMedicare Group PPO & BlueMedicare Group HMO Products	\$200 per contract annually	\$100 per contract annually
BlueMedicare Group Rx (PDP)	\$50 per contract annually	N/A

\* These products are separate and distinct from Over 65 Medicare Advantage and Part D products.

- Group Retiree commissions are paid at the time of new sale and on the group's annual renewal date.
- No adjustments for contracts added or terminated after the new sale or renewal effective month will be paid.

## Blue Vision Commissions

BluePartners Classification	% of Reconciled Premium	
	With a GA	Without a GA
Blue Diamond Blue Preferred Blue Standard Plus	8%	10%
Blue Standard	6%	8%

- Blue Vision commissions are paid monthly based on reconciled premiums.

## Commissions for Other Products

Commissions for other products not set forth in this Addendum will be paid according to the then-current compensation schedule for the other product, subject to the Agent's compliance with the applicable Florida Blue policies and procedures.

## FLORIDA COMBINED LIFE INSURANCE COMPANY, INC. (FCL) COMMISSION SCHEDULE

The ancillary products listed below are offered by Florida Combined Life Insurance Company, Inc. (FCL). FCL is an affiliate of Florida Blue and an Independent Licensee of the Blue Cross and Blue Shield Association.

### GROUP DENTAL

Annualized Premium Per Group	Blue Dental Choice & Voluntary (Fully Insured)	Blue Dental Care Prepaid Group & Voluntary
Up to \$10,000	10.00%	10.00%
Up to the next \$10,000	8.00%	10.00%
Up to the next \$10,000	6.00%	10.00%
Up to the next \$20,000	4.00%	10.00%
Up to the next \$200,000	2.50%	10.00%
Up to the next \$250,000	2.00%	10.00%
Up to the next \$2,000,000	1.50%	10.00%
Over \$2,500,000	1.00%	10.00%

- Commissions may be adjusted at renewal or off-anniversary due to factors including but not limited to: additions, cancellations or modification of benefits of any product or fluctuation in enrollment or premium volume.

### GROUP LIFE AND DISABILITY

Number of Enrolled Lives	Group Life & Disability	Voluntary Life & Disability
4 - 50	15.00%	15.00%
51 - 300	12.00%	15.00%
301 – 500	9.00%	15.00%
500+	7.00%	15.00%

## Addendum B: Agency “Good Standing” & Reappointment Requirements

In order for an Agency to remain in good standings with the Company and maintain Appointments for its Designated Producers as Appointed Agents for Company, an Agency:

1. Must comply with the terms and conditions of the Agency Agreement.
2. Must comply with all Florida Blue of Florida and its subsidiaries and affiliates, corporate policies and procedures.
3. Designated Producers must have active inventory of a minimum of five (5) Group Cases or fifty (50) Group Contracts (for the purposes of this Addendum B, the “minimum inventory standard”) (“cases and contracts” refers to accounts sized four (4) or greater) which inventory will be evaluated:
  - i. At the end of the initial twelve (12) month period calculated from the date of appointment; and
  - ii. At the end of every subsequent twelve (12) month period thereafter.
4. For each Designated Producer of Agency who satisfies the minimum inventory standard, Company will pay to renew the Appointment of such Designated Producer; however,
  - i. If a Designated Producer does not satisfy the minimum inventory standard, the Agency shall, within thirty (30) calendar days, reimburse Company for the Appointment Fees Company paid on behalf of such Designated Producer.
  - ii. If a Designated Producer does not satisfy the minimum inventory standard at the time of appointment renewal, the Agency shall pay for the fees to renew such Designated Producer’s Appointments, if applicable.
  - iii. If a Designated Producer’s Appointment is terminated by the State of Florida for any reason, the Agency shall, within thirty (30) calendar days, reimburse Company for the Appointment Fees Company paid on such Designated Producer’s behalf and Agency shall pay the fees to renew such Designated Producer’s Appointment, if applicable.
  - iv. In the event Agency fails to reimburse Company or submit renewal Appointment Fees, Company shall, within thirty (30) calendar days, terminate Appointment(s) for Agency’s Designated Producer(s), which did not meet the requirements of #4, and, if applicable, retract any Appointment fees owed from commissions.
5. Designated Producers must have a valid Florida resident health and life agent license.
6. Must have on file with Company a fully executed Agency Agreement.
7. Designated Producers must have on file with Company a fully executed Designated Producer Addendum.
8. Must provide evidence of Errors and Omissions insurance coverage, minimum acceptable coverage is \$500,000 per occurrence and \$1,000,000 in aggregate, and must maintain such insurances for the duration of their Appointment with the Company.
9. Must provide evidence that all continuing education credits/coursework requirements have been met by Designated Producers.
10. Must have information systems capabilities to include Internet access to facilitate email communication and other electronic tools, such as “e-quotes” and electronic enrollment. Please refer to Addendum “D” for further explanation of the information systems requirements for Agency.

**SECTION 2:  
OPERATING SYSTEM AND HARDWARE REQUIREMENTS  
JANUARY 1, 2025 – DECEMBER 31, 2025, CALENDAR YEAR**

Listed below are the designated operational system requirements for optimal site performance under the technology platform used by Florida Blue. In order for your Agency to take advantage of all of the capabilities that Florida Blue has designed and implemented, and in order for your Agency to remain designated as an Appointed Agency in Good Standing, your Appointed Agency must:

1. Enroll for Electronic Funds Transfer (EFT) with Florida Blue to receive payment of commissions due.
2. Adopt the operational systems requirements that are mentioned in this Addendum.

**The operational system requirements are:**

<b><i>Browser</i></b>	Chrome up to version 124.0 or above (Preferred)
<b><i>Adobe Acrobat Reader</i></b>	2024 or above
<b><i>Screen Resolution</i></b>	1024 x 768 or higher

Florida Blue reserves the right to make modifications or perform upgrades to its computer systems and sales platforms. Therefore, from time to time, Florida Blue may issue revised Operating and Hardware Requirements to Appointed Agencies in order to enable Appointed Agencies' systems to achieve the desired level of performance in light of any such upgrades or modifications.

Florida Blue Appointed Agencies are required to implement such electronic payment processes as Florida Blue shall determine. Printed or paper commission checks are not available.

## EXHIBIT D

### AGENCY SECURITY REQUIREMENTS

#### 1. DEFINITIONS

Capitalized terms not otherwise defined in this Exhibit (Agency Security Requirements) have the respective definitions assigned to them in other parts of the Agreement.

**“Agreement”** refers to one or more contractual business arrangements between the parties for providing certain services for Companies which may involve Agency’s acquisition, retention, creation, transmission, use and/or disclosure of Protected Health Information on behalf of Companies.

**“Applicable Law”** is all Federal and State laws and regulations that apply to the privacy and security of Companies PI.

**“Agency Custody”** is defined as when the Companies’ PI: (i) physically resides on Agency’s network; (ii) passes through Agency’s network to Companies; or (iii) remains on Companies’ network and Agency only has controlled access to the Companies’ PI, through a presentation layer.

**“DMZ”** is defined as a computer host or small network inserted as a “neutral zone” between a company's private network and the outside public network.

**“Effective Date”** is the last execution date of the Agreement containing this Exhibit”.

**“Companies PI”** is all Protected Information (PI) that is, pursuant to the Agreement:

- i. disclosed by Companies to Agency; or
- ii. otherwise received, maintained, used, or created by Agency on behalf of Companies.

PI includes all personally identifiable information protected under various state and federal statutory and regulatory requirements including, but not limited to, Gramm-Leach-Bliley (**“GLB”**) for financial information, as well as any other applicable federal or state restrictions on personally identifiable information, such as the Florida Information Protection Act (collectively **“Applicable Law”**). Information transmitted or maintained electronically, orally, on paper or other media is covered.

**“Mobile Devices”** is removable media capable of storing information such as, but not limited to, universal serial bus (USB) drives, mp3 players, SD Cards, CD’s, ZIP drives, Laptops, personal digital assistants (PDA’s), smart phones, cameras, and camera phones.

**“Security Incident”** is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

**“Agency Personnel”** is defined as Agency’s employees, agents, independent contractors, subcontractors, or Third Parties who are authorized to access Companies PI.

**“Third Party”** is defined as any entity not a party to this contract that uses, accesses, stores, processes, and/or gathers PI on behalf of the Agency.

#### 2. COMPLIANCE WITH SECURITY REQUIREMENTS

- (a) Agency represents and warrants it is in compliance or at its cost will implement the

security measures set forth herein and maintain documentation confirming such implementation. Such documentation will be made available upon the request of Companies.

- (b) Failure of Agency to materially comply with the provisions and requirements of this Exhibit will entitle Companies to terminate the Agreement immediately, or to not process transactions from Agency until such time as any or all non-compliance is cured to the reasonable satisfaction of Companies at Companies' sole discretion.
- (c) Within thirty (30) days of the Effective Date, unless documented herein, Agency will provide Companies with a detailed written notification of any and all instances of Agency non-compliance with the requirements described in this Exhibit, as well as a summary of corrective actions to achieve compliance with each outstanding requirement.
- (d) Agency will implement the corrective actions identified in 2(c) within the first year following the Effective Date, or within such lesser time as may be mandated by Companies, in Companies' reasonable discretion.
- (e) Agency will provide immediate notification should Agency become non-compliant during the period of the Agreement, as well as a summary of corrective actions to achieve compliance with each outstanding requirement. Such corrective action will be completed within a mutually agreed upon time frame. Companies has the right to not process transactions from Agency until such time as any or all non-compliance is cured to the reasonable satisfaction of Companies.
- (f) Agency will maintain adequate documentation to demonstrate compliance with this Agreement for a minimum of five (5) years or longer if required by Applicable Law, and will provide copies of such documentation to Companies upon request.
- (g) Agency will require that all Third Parties comply at a minimum with no less restrictive security requirements than those set forth herein.

### **3. SAFEGUARDING PROCEDURES**

- (a) Agency shall establish and maintain physical, technical, administrative, environmental, safety and facility procedures; data security procedures and other safeguards against the destruction, loss, theft, unauthorized disclosure, access, or alteration of Companies PI in the Custody of Agency. Agency's procedures and safeguards shall be documented in an Information Security Program. Such procedures and safeguards shall, at a minimum:
  - (i) follow the industry best practices for security systems, computers and technologies, including firewalls and encryption;
  - (ii) be no less rigorous than those maintained by Agency for its own information of a similar nature or for other customers of Agency with respect to information of a similar nature;
  - (iii) meet the requirements of Applicable Law; and
  - (iv) include all of the controls required by this Exhibit.
- (b) Agency shall provide Companies with downloads of Companies PI in the Custody of

Agency, as requested by Companies.

- (c) Agency shall continuously monitor and periodically, but no less than annually, evaluate and test its Information Security Program. Agency shall promptly adjust and/or update such program as reasonably warranted by information security threats.

#### **4. DATA ACCESS**

- (a) **“Agency Data Files”** includes all computer or other files to the extent such computer or other files contain or control access to Companies PI, as well as all systems, network logs, system parameters, and other documentation to the extent that such systems, logs, parameters, and other documentation contain or control access to Companies PI.
- (b) Upon the request of Companies, Agency shall provide copies of Agency Data Files to Companies. Agency shall also confirm in writing that all Agency Data Files are complete and that no part of such Agency Data Files has been deleted, withheld, disguised or encoded in a manner inconsistent with the purpose of evaluating Agency’s compliance with Applicable Law, this Exhibit, and/or the Agreement. Agency may redact all data pertaining to Agency’s other clients.
- (c) Agency will only grant access to use or copy Companies PI at authorized locations.
- (d) Agency will only grant access to Companies PI as part of a documented process. Such process shall limit access to the minimum necessary access to achieve the intended purpose. If Companies PI is PHI, the minimum necessary restrictions shall meet the requirements of CFR 164.514(d)(1).
- (e) Agency shall perform background checks on Agency Personnel with a need to access Companies PI prior to giving such Agency Personnel access to Companies PI. Agency shall provide documentation of compliance upon request of Companies and before any access by Agency Personnel to any Companies PI.
- (f) Companies PI must not be processed, loaded, used or otherwise placed in Agency’s test, development or non-production environments.
- (g) Agency will review access to Companies PI to ensure access has only been granted to authorized Agency Personnel:
  - (i) at least once every twelve (12) months for Companies PI in Agency’s Custody; and
  - (ii) at least monthly for all Agency Personnel that have been issued credentials to access Companies systems.
- (h) Agency will immediately remove access to Companies’ PI from Agency Personnel that no longer require access to Companies PI in Agency’s Custody and/or immediately notify Companies if Agency Personnel no longer require access to Companies systems.

#### **5. DATA STORAGE**

- (a) Agency will segregate Companies PI in Custody of Agency from information of Agency’s other clients and customers so that such information is not commingled.
- (b) Companies PI in the Custody of Agency will be encrypted at rest using a minimum of

Advanced Encryption Standard (AES) 256. In cloud and server environments, the cypher key must be unique to Companies.

## **6. CERTIFICATION**

- (a) Within one (1) year after the Effective Date, and at Agency's expense, Agency will earn a mutually agreed upon information security certification from a firm that specializes in enterprise information security assessment and certification. Agency will maintain the certification for the entire duration of the Agreement. The preferred certification program is a properly scoped annual SOC 1 or 2, Type II review that includes assessment of the entire IT infrastructure that supports the Services provided by Agency and related security policies and practices. If a SOC 1 is submitted it must cover all the relevant control objectives required for the Model Audit Rule. Copies of all security attestations held must be submitted to Companies upon renewal of the certification.
- (b) At or before signing the Agreement Agency will complete Companies' Agency Security Certification (ASC). Thereafter, upon Companies' request, but no more than annually, Agency will complete and sign an ASC attesting to Agency's compliance with the items in this Exhibit, and return such form to Companies.

## **7. COMPANIES PI SHARING OR TRANSFER**

- (a) Agency will obtain written authorization from Companies at least thirty (30) days prior to:
  - (i) the first instance of any recurring, one-time and/or non-recurring offshoring of Companies PI; and
  - (ii) the first instance of any recurring, one-time, and/or non-recurring sharing or transfers of Companies PI to Agency's affiliates or to Third Parties;
- (b) When sharing Companies PI with Third Parties, Agency will maintain an instance specific accounting of all Companies PI that includes the following:
  - (i) the date the Companies PI was shared;
  - (ii) the recipient of the Companies PI;
  - (iii) a description of the Companies PI;
  - (iv) the individuals whose PI was shared; and
  - (v) the reason the Companies PI was shared.
- (c) For all network-based transfers between Companies and Agency involving Companies PI, Agency will use secure transmission methods (including but not limited to, private circuits, frame relay connections, virtually private encrypted connections, or encrypted information transfer protocols) and Single Sign On, as agreed upon by Companies and Agency.
- (d) For all network-based transfers between Agency and any Third Party, Agency will only transfer Companies PI:
  - (i) via a private network between Agency and the other Third Party (such as a

- private circuit or frame relay connection);
  - (ii) if sent over the open Internet, via a wholly encrypted communication tunnel (such as Local Area Network (LAN) to LAN Virtual Private Network (VPN));
  - (iii) if sent using File Transfer Protocol (FTP), via an encrypted information transfer protocol; or
  - (iv) via HTTPS with a minimum certificate length of 2048.
- (e) If Agency is authorized to electronically receive, collect, transmit, or disclose Companies PI on behalf of Companies, Agency will only do so using encrypted information transfer protocols, as agreed upon with Companies.
  - (f) Agency will utilize secure protocols (including, but not limited to Secure FTP, Secure Shell (SSH), and/or Secure Socket Layer (SSL) in place of standard FTP, standard Telnet, and HTTP) to move or transfer Companies PI over internal networks owned and/or operated by Agency.
  - (g) Agency will handle collection and transfers of non electronic Companies PI securely as mutually agreed upon in writing between the parties.
  - (h) When using email to transmit Companies PI externally, Agency must use encrypted email.

## **8. BACKUP REQUIREMENTS FOR COMPANIES PI IN AGENCY'S CUSTODY**

- (a) Agency will make backup copies of Companies PI in accordance with a documented backup plan developed by Agency that includes, at a minimum, the requirements of this Agreement.
- (b) Agency will, at a minimum, do full backups weekly with incremental backups occurring daily.
- (c) Where Agency uses offsite backup facilities (including offsite vaulting services through a Third Party) as part of its backup plan, Agency will encrypt all Companies PI stored on backup media and the encryption key will be stored separately from the media at all times.
- (d) All backup media will be stored in a secured area accessible only by authorized individuals.
- (e) Where Agency maintains its own backup media as part of its backup plan, Agency will maintain a log of all parties entering/exiting the area where the backup media is kept. Additionally, Agency will implement a process and procedure for conducting monthly log reviews for persons entering the area.
- (f) Where Agency outsources media storage services as part of its backup plan, Agency will require the applicable vaulting service to maintain a log of all parties entering/exiting the area where the backup media is kept. Agency will encrypt all electronic Companies PI stored with Third Parties and the encryption key will be stored separately from the media at all times.

## **9. DISPOSAL OF LINGERING COMPANIES PI IN AGENCY'S CUSTODY**

- (a) Agency will promptly remove electronic Companies PI from temporary locations controlled by Agency (such as, but not limited to, laptops, workstations, web servers, FTP servers, or database servers) after the intended business purpose has passed.
- (b) Agency will remove all electronic Companies PI from any storage media prior to disposal, utilizing the methods described by the National Institute of Standards and Technology (NIST) to clear, purge or destroy the storage media. Agency will document the disposal of any hardware or media (such as, but not limited to tape drives, thumb drives, diskettes, compact discs (CD's), digital video discs (DVD's), laptop drives, workstation drives, or server drives) storing Companies PI. At a minimum, the documentation shall include equipment description, serial numbers, dates of disposal, reason for disposal, method of disposal, and individuals performing the disposal. A NIST certificate of destruction is to be provided to Companies annually.
- (c) Agency will dispose of all other Companies PI by shredding, erasing, or otherwise modifying the Companies PI to make it unreadable or undecipherable through any means.

## **10. TRAINING**

- (a) If Agency has Custody of Companies PI, Agency Personnel will take Companies security and privacy training. If Agency has Custody of Companies PI, Agency Personnel will take Agency's security and privacy training. Agency's security and privacy training shall, at a minimum, cover compliance with Agency's obligations and restrictions under this Agreement, with Applicable Law, and with Agency's Information Security Program.
- (b) Agency Personnel that have access to Companies PI must complete security and privacy training at least once every twelve (12) months.
- (c) Such training shall be documented by both Companies and Agency for Custody and by Agency for Custody of Companies PI, including a record of those individuals who received the training, when they received it, and source of training (Companies or Agency).

## **11. WIRELESS**

- (a) If Companies PI is accessible wirelessly by authorized Agency Personnel, the following minimum security configuration standard shall be implemented by Agency for the wireless network:
  - (i) strong encryption (AES-128 at a minimum) must be utilized;
  - (ii) the wireless LAN must be segmented from the wired network utilizing a firewall; and
  - (iii) once wireless access is established, additional authentication of authorized Agency Personnel must be performed prior to allowing access to wired LAN resources.
- (b) Any built-in wireless technologies in end point devices must be set for manual connection unless the network is protected as described in clause (a) above.
- (c) Wireless features on Agency desktops and laptops must be disabled whenever they are

connected to Agency's wired LAN.

## **12. LOGGING AND MONITORING**

- (a) Agency will log and monitor access to Companies PI.
- (b) Agency will develop, implement, and adhere to a log retention policy requiring that system activity and user access logs be kept for a minimum of one (1) year, and logs associated with Security Incidents be kept for six (6) years.
- (c) Agency will have an effective monitoring program for oversight of Agency Personnel providing Services or working on Companies systems and programs.

## **13. INTRUSION PREVENTION AND DETECTION**

- (a) Agency will implement a network-based intrusion detection system (IDS) or intrusion protection system (IPS) solution on all network segments containing systems accessing, storing or processing Companies PI.  
  
and/or
- (b) Agency will implement a host-based IDS or IPS solution on all hosts accessing, storing or processing Companies PI.

## **14. AUTHENTICATION AND PASSWORDS**

- (a) Agency will adhere to a documented industry standard identity verification process.
- (b) Agency will use separate IDs and passwords for privileged and non-privileged access.
- (c) Agency will incorporate the following requirements into their account password policy for all systems (including, but not limited to, hardware and software) accessing, storing or processing Companies PI:
  - (i) requires password complexity where technically possible;
  - (ii) requires frequent password changes (maximum of every ninety (90) calendar days between changes);
  - (iii) requires that a password history be configured to prevent passwords from being reused within the prior twelve (12) months at a minimum;
  - (iv) invokes an account lock-out after five (5) consecutive failed attempts at a maximum;
  - (v) requires an administrator or automated challenge response system to verify the user's identity prior to reinstating the account; and
  - (vi) inactive accounts are disabled or deleted.
- (d) Under no circumstances will user names in conjunction with passwords associated with accounts that allow access to Companies PI be shared or transferred among Agency Personnel or with any other person.

## **15. INFRASTRUCTURE ARCHITECTURE**

- (a) Agency shall not store any Companies PI on a device located on a DMZ segment. The data must be stored on an internal segment and accessed by the application layer of the application providing such access. Virtual environments can be used, but must maintain the separation described above (i.e., cannot have DMZ and Internal virtual hosts on the same physical device).
- (b) If Agency makes Companies PI available to public-facing entities (Internet, B2B, etc.):
  - (i) a dedicated switch for DMZ hosts must be utilized (not shared with systems located on other segments);
  - (ii) the switch must have all ports disabled that are not in use;
  - (iii) the switch must have port level security enabled to disable the port when the device is unplugged and also to prevent other systems from being plugged into a port by accident;
  - (iv) each hosted application component (web, application and database) must reside on its own environment, totally isolated from one another via firewall interfaces (i.e., a separate firewall or separate ports in a single firewall);
  - (v) port level restrictions (access control lists) must be in place at each firewall interface allowing only required ports inbound/outbound to/from each layer (source/destination IP/ports where possible with all other traffic denied); and
  - (vi) systems located on the outer-most DMZ segment (web layer) must not be permitted to initiate outbound communications to non-trusted networks (Internet, etc.).

## **16. PATCH MANAGEMENT**

- (a) Agency will adhere to a documented industry standard patch management process for all aspects of Agency's environment.
- (b) Agency will apply applicable critical security patches or other risk mitigation measures within twenty four (24) hours.
- (c) Agency will apply applicable non-critical security patches or other risk mitigation measures on at least a quarterly basis.

## **17. VULNERABILITY SCANNING AND PENETRATION TESTING**

- (a) Agency will adhere to documented industry standard vulnerability scanning policies and procedures.
- (b) Agency will conduct vulnerability scans at least annually or on a quarterly basis for PCI data:
  - (i) on any equipment that accesses, stores and/or processes Companies PI;
  - (ii) on non- Companies devices that share common network resources with the equipment described above in (i); and

- (iii) on all Internet-facing applications that access, store or process Companies PI prior to production implementation to verify that all applicable Open Web Application Security Project (OWASP) Top 10 and SANS Top 20 vulnerabilities have been prevented, or are PCI compliant;
- (c) Within the first year of this Agreement, and annually thereafter, Agency will engage a third party to conduct penetration testing against Agency's infrastructure. Summary findings and remediation results that could impact Companies PI must be shared promptly with Companies.
- (d) Vulnerabilities identified during scanning or penetration testing must be fixed or other risk mitigation measures put in place within twenty-four (24) hours for critical findings and no more than ninety (90) days for lesser findings.

## **18. WEB HOSTING**

(a) For hosting arrangements in which Companies users (including, but not limited to, customers, employees, etc.) access Agency's website, upon completion or time out of a session, Agency will automatically log out and redirect that user to a log-off page or other site agreed upon by Agency and Companies.

## **19. SOFTWARE**

- (a) All Agency Personnel will be prohibited from installing any software not pre-approved by Agency's software management policy on any hardware that may access, store, or process Companies PI.
- (b) Agency will not implement keystroke monitoring software/hardware on systems processing and/or storing Companies PI unless mutually agreed upon in writing.

## **20. DEVICE AND HOST CONFIGURATION CONTROLS**

- (a) If applicable Agency will harden operating systems, utilizing the least amount of services required.
- (b) Agency will implement Virus Protection as follows:
  - (i) All hardware used to conduct business for Companies must have current antivirus software protection installed; and
  - (ii) All hardware used to conduct business for Companies must have up-to-date virus definitions, updated at least once per day.
- (c) Agency will implement Automatic Lockout for electronic sessions on any hardware (i.e., laptops, workstations, mobile devices, servers, etc.) that access, store, or process Companies PI. The screen and/or console will lock after thirty (30) minutes of inactivity at most and require the user to re-authenticate.
- (d) PCs used to process Companies PI will be dumb terminals, thin clients that do not locally process data or execute user programs, or have data loss prevention controls in place.
- (e) Printers cannot be accessed from hardware used to store or display Companies PI, or else access is controlled.

**21. MOBILE DEVICES [NOTE: AGENCY WILL HAVE THE OPPORTUNITY TO CHOOSE WHICH “A” OPTION: FIRST “A” ALONE; OR SECOND “A” PLUS B-D]**

- (a) Mobile Device drives or access ports are not part of the end point configuration.

**or**

- (a) Agency will limit the use of Mobile Devices by Agency or Agency Personnel to only media owned or supplied by Agency.
- (b) Agency Personnel will not connect personally owned Mobile Devices to any hardware that is used to conduct business for or on behalf of Companies.
- (c) Agency will encrypt, using an Agency corporate solution, any and all Mobile Devices used for storage of Companies PI. The encryption software must utilize at least AES-128 encryption and encrypt the entire removable device (all partitions), and it must not allow the option of individual folder and/or file level encryption.
- (d) any and all Mobile Devices used for storage of Companies PI must be transported in a secure manner including but not limited to, as carry-on (hand) baggage when using public transportation and must be concealed and/or locked when in an unattended private vehicle (e.g., locked in the trunk of an automobile).

**22. REMOTE ACCESS**

**(a) Remote Access to Agency’s Internal Network.**

- (i) For all remote access to Agency’s internal network for any reason, traffic with the remote device must be encrypted and the remote user must utilize strong authentication (authentication and password requirements listed in AUTHENTICATION AND PASSWORDS section above apply).
- (ii) Agency shall have policy and/or technical controls covering acceptable use of remote access from a public location (e.g., airports, coffee shops, etc.).

**(b) Remote access to Companies’ Network.**

- (i) Agency understands and agrees that remote users can only connect using remote display technologies as specified by Companies.
- (ii) Agency Personnel will not access the Companies network from public spaces in which unauthorized persons are present (including, but not limited to, airports, coffee shops, etc.) or shall have policy and/or technical controls covering acceptable use of remote access from a public location.
- (iii) Agency agrees that users will maintain an active connection only for the required time and purpose and will disconnect when the user no longer requires an active connection. Agency is responsible for all activity that occurs during the connected session.
- (iv) Agency Personnel will not print, download, email, or otherwise copy Companies PI to destinations outside of the Companies network, unless allowed in the Agreement or a Statement of Work (“SOW”). Destinations outside of the Companies network include, but are not limited to, personal email accounts, non-

Companies owned devices including printers, computers, personal digital assistants, cell phones, portable storage devices, etc.

- (v) In addition to the requirements in the Agreement or a SOW, Agency will sign and comply with the terms and conditions of Companies' Remote Access Approval Package.

**(c) Agency At Home Resources (AHRs)**

- (i) An "At Home Resource" ("AHR") is an Agency personnel resource who regularly performs their functions involving the Companies' PI, remotely or otherwise outside the Agency's physical facilities or office locations.
- (ii) AHRs are subject to the requirements of section 20(b) Remote access to Companies' Network above.
- (iii) Agency will prevent the AHR from migrating data out of the remote display session, except as agreed upon. Hardware configuration controls to prevent this will include, at a minimum:
  - a. PCs with data loss prevention controls, or thin client devices that must be physically tethered (connected) with an Ethernet cable. No printer, wireless or email capability is available on the machine;
  - b. USB Softphone, if phone capability is necessary; and
  - c. Headsets via USB plug, if headsets are necessary.
- (iv) If AHRs are required under a Companies Agreement or SOW to be PCI compliant, AHRs as a group must be listed in the Agency's PCI attestation.
- (v) Agency will adhere to documented policies and procedures for at home access. Those policies and procedures must include at a minimum:
  - a. AHR must work in a segregated area away from other inhabitants of the house. At no time will an AHR perform Services on behalf of Companies within the general population of the house;
  - b. Recording devices and use of cameras for screen capture are prohibited;
  - c. All hardware utilized by the AHR is provided by, and is the property of the Agency, and must not be modified, or the hardware utilized by the AHR must have software installed that provides an equivalent level of security;
  - d. Clean desk policy for AHR; and
  - e. Penalties for noncompliance.
- (vi) Work From Home Agreements must be signed by all AHRs that include compliance with the policies and procedures for working at home and include the right for a physical at home audit conducted by the Agency and/or Companies.

- (vii) The Agency must have an effective AHR oversight program. The program must include audits of the AHR against the policies and procedures defined above, including visits to the AHR's home. The audits must cover a significant portion of the population of AHRs.
- (viii) AHRs must be located in the United States and not offshore.

## **23. PHYSICAL SECURITY PLAN**

- (a) Agency will maintain and follow appropriate physical security procedures, including, but not limited to, regular monitoring of all work areas, secure business facilities, data centers, paper files, servers, back-up systems, and computing equipment, including all mobile devices and other equipment with information storage capability.
- (b) Agency will limit physical access to work areas and to systems that may access, store, or process Companies PI to only those Agency Personnel that have a business need for such access.
- (c) Agency will document all physical security controls at least annually, or following significant moves or building additions, and will supply such documentation to Companies for review, upon Companies' request, or prior to such move or building addition.
- (d) Agency will include the following physical security controls in locations where Companies PI is stored and/or accessed:
  - (i) electronically controlled access, restricting access to only those with a business need;
  - (ii) establish a clean desk policy for staff, with no phones, paper, purses, or cases; and
  - (iii) cameras with recording capability at all entrances. Recordings will be maintained for a minimum of 90 days.

## **24. SECURITY INCIDENTS**

- (a) Agency will report any Security Incident involving the confidentiality, integrity, or availability of Companies PI, including, without limitation, customer facing outages, loss of information, degradation of information integrity, identity theft, compromise of user account(s) or password(s), malicious code infection spreading via an automated mechanism, or virus outbreaks experienced by Agency promptly, but no later than twenty four (24) hours) after such Security Incident, or sooner if reasonably necessary given the circumstances.
- (b) The Parties mutually agree that as to Unsuccessful Security Incidents (as defined in the most recent Business Associate Agreement between the parties) that do not result in unauthorized access, use, disclosure, modification, or destruction of EPHI, or interference with an information system, this paragraph constitutes notice by Agency of Unsuccessful Security Incidents. Agency will provide a summary report of Unsuccessful Security Incidents of which Agency becomes aware on at least an annual basis.

## **25. BUSINESS CONTINUITY**

(a) Agency will have business continuity plans in place to ensure that the goods and/or Services contracted for by Companies will be delivered in accordance with schedules agreed to by both parties. These plans should address the performance failure of Agency's subcontractors.

## **26. SECURITY AUDIT RIGHTS**

Companies has the right to perform an audit at Agency's site including, but not limited to, an on-site visit and inspection of physical security measures, data security measures, status of third party certifications, compliance with this Exhibit, compliance with HIPAA requirements and other Applicable Law, and the condition of Agency's facility. Companies will provide Agency with a fifteen (15) day advance notice of such site audit. Companies will conduct the site audit during normal business hours, and the site audit will not be intrusive. Companies will conduct no more than one audit in a twelve (12) month period, or after a Security Incident, whichever is shorter, unless a site audit reveals security risks. Each party will bear its own costs for each annual audit. If a discovered security risk necessitates a re-inspection, then Agency will reimburse Companies for all reasonable costs incurred during such re-inspection.

