AMENDMENT TO BROKERAGE AGREEMENT – LAST UPDATED: 3/15/2019

This AMENDMENT TO THE BROKERAGE AGREEMENT ("Amendment") is made effective March 1, 2019 (the "Effective Date") by and between Broker ("Broker") and Principal ("Principal"). The Broker and Principal are collectively referred to herein as "Parties". This Amendment can be found on the GuardianLife.com website or via your Principal.

WHEREAS, the Parties have previously entered into a Brokerage Agreement, including any exhibits, schedules and amendments thereto (collectively, the "Agreement"); and

WHEREAS, the Parties desire to amend the Agreement; and

WHEREAS, the Parties agree that this Amendment is incorporated into, and made a part of, the Agreement;

NOW, THEREFORE, the Parties agree as follows:

1. The above introductory paragraph and WHEREAS clauses are incorporated herein by reference;

2. The Agreement is hereby amended by adding to the Agreement security and privacy requirements, a business associate agreement, and rules and requirements governing the use of alternative group enrollment technology platforms, as follows:

   A) Security and Privacy Requirements. The Security and Privacy Requirements for Brokers (Exhibit A to this Amendment) are incorporated into, and made a part of, the Agreement.

   B) Business Associate Agreement. The Business Associate Agreement for Brokers (Exhibit B to this Amendment) is incorporated into, and made a part of, the Agreement.

   C) Rules and Requirements Governing Use of Alternative Group Enrollment Technology Platforms. Use of Alternative Group Enrollment Technology Platforms (Exhibit C to this Amendment) is incorporated into, and made a part of, the Agreement.

3. **Full Force and Effect.** Other than as specifically amended by this Amendment, the provisions of the Agreement shall remain in full force and effect.

4. **Defined Terms.** Capitalized terms used in this Amendment and not otherwise defined shall have the meanings ascribed to them in the Agreement.

5. **Conflict.** In the event of any conflict between this Amendment and the Agreement, this Amendment shall prevail.

This Amendment (including, without limitation, all Exhibits hereto) is hereby effectuated by general announcement pursuant to the Amendments section of the Brokerage Agreement. Neither assent nor signature by Broker is required.

List of Exhibits

Exhibit A – *Security and Privacy Requirements for Brokers*

Exhibit B – *Business Associate Agreement for Brokers*

Exhibit C – *Use of Alternative Group Enrollment Technology Platforms*

Exhibit A to Brokerage Agreement Amendment Effective March 1, 2019
Security and Privacy Requirements for Brokers
LAST UPDATED: 3/15/2019

These Security and Privacy Requirements for Brokers ("Security and Privacy Requirements") are incorporated into, and made a part of, the Brokerage Agreement to which you are a party ("Agreement") and can be found on the GuardianLife.com website (the "Site") or via your Principal. Capitalized terms used herein without definition shall have the meaning ascribed to them in the Agreement unless otherwise specified herein. During the time Broker is in possession of, or has access to, any Nonpublic Information, Broker: shall comply with all of the requirements set forth in these Security and Privacy Requirements; and shall not diminish the security safeguards in effect as of the effective date of the Agreement. In the event of any conflict between these Security and Privacy Requirements and the provisions of the Agreement or any Business Associate Agreement by and between the parties, the provisions of these Security and Privacy Requirements and said Business Associate Agreement, respectively, will govern. In the event of any conflict between these Security and Privacy Requirements and the provisions of any Business Associate Agreement by and between the parties, said Business Associate Agreement will govern.

These Security and Privacy Requirements may be modified, supplemented or amended at any time and for any reason. Any such changes that are posted on the Site from time to time are hereby expressly incorporated herein by reference. We will alert you about any changes by updating the "LAST UPDATED" date (shown above) of these Security and Privacy Requirements. It is your responsibility to periodically review the Site for any changes to these Security and Privacy Requirements to stay informed of updates. You will be subject to, and will be deemed to have been made aware of, and to have accepted, any changes to these Security and Privacy Requirements as of the date such revised Security and Privacy Requirements are posted.

1. **Definitions.**

"Data Protection Laws" means all laws or regulations relating to data protection, privacy and the interception, recording or monitoring of communications which are deemed to include, but are not limited to: the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 ("**HIPAA**"), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (the "**HITECH Act**"), New York Department of Financial Services, Cybersecurity Requirements for Financial Services Companies 23 NYCRR 500 ("**NY-DFS**"), the New York Information Security Breach and Notification Act and the Gramm-Leach-Bliley Act of 1999, and any other applicable federal, state or local laws or regulations whether or not such laws or regulations directly apply to Broker.

"Nonpublic Information" means all Guardian and/or Principal information, regardless of format, that is not Publicly Available Information (as defined by applicable law) and is:

a. Business-related information of Guardian or Principal, the tampering with which, or unauthorized disclosure, access or use of which, could cause a material adverse impact to the business, reputation, operations, or security of Guardian or Principal; or

b. Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, alone or in combination with any one or more of the following data elements: (i) Social Security number, (ii) driver's license number or non-driver identification card number, or passport number (iii) account number, insurance policy number, credit or debit card number, (iv) any security code, access code or password or password challenge questions or answers that could permit access to an individual's financial or other account, (v) date of birth or (vi) biometric records; (vii) genetic information or records; (viii) signature; (ix) street address, email address or telephone number; (x) mother's maiden name; or

c. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or a member of the individual's family or (iii) claims or payment for the provision of health care to any individual or a member of the individual's family; or

d. Any information covered by Data Protection Laws.

"Security Event" means any act, successful or unsuccessful, to gain unauthorized access to, or disrupt, misuse, tamper with, or alter, any Nonpublic Information. For this purpose, "unauthorized access" includes, without limitation, both a security breach of Service Provider's systems and a security breach of any systems of any of Broker's subcontractors or other third parties to which Broker provides access to, or that stores or processes, any Nonpublic Information.

2. **Security Program Overview.** Broker shall develop, implement and maintain a written security program that includes administrative, technical and physical safeguards that are appropriate to the nature and scope of its activities performed for Guardian or Principal and the sensitivity of Nonpublic Information.

Such safeguards shall be reasonably designed to:

a. Ensure the security and confidentiality of Nonpublic Information;
b. Identify and protect against threats or hazards to the security, availability or integrity of Nonpublic Information;
c. Protect against and detect unauthorized access to, or use of, Nonpublic Information; and
d. Comply with all legal and regulatory requirements applicable to Nonpublic Information.

Broker shall utilize qualified technology and cybersecurity employees or services to undertake such responsibilities.

3. **Service Provider Requirements.** Without limiting the foregoing, Broker shall, as part of its security program, perform appropriate actions, including, but not limited to, overseeing its service providers, by:

a. Taking reasonable steps to select and retain service providers that are capable of maintaining their own safeguards for Nonpublic Information that are no less stringent than the requirements set forth in these Security and Privacy Requirements;
b. Requiring its service providers by contract to implement and maintain such safeguards; and
c. Monitoring its service providers, including by periodic assessment, to confirm that they have satisfied their obligations to protect Nonpublic Information as required by these Security and Privacy Requirements.

4. **Personnel, Policies and Procedures.** If any personnel or subcontractors of Broker are provided with access to any Guardian or Principal systems or facilities, Broker shall ensure that any such persons shall comply with (i) all applicable policies and processes of Guardian that Guardian or Principal communicates to Broker and (ii) these Security and Privacy Requirements. Broker shall ensure that such persons do not access or attempt to access any computer system, electronic file, software, or other electronic services other than those specifically required to perform its obligations under the Agreement.

5. **Security Event, Notification and Investigation.** Broker shall immediately, but in no event more than 24 hours, notify Principal and Guardian at 212-919-8800 (select option: Report an Information Security Incident) of any Security Event. Such notification shall include a detailed description of the Nonpublic Information at issue and the factual circumstances surrounding such Security Event. Broker shall cooperate with Guardian and Principal and shall promptly provide Guardian and Principal with information, to the extent such information is known to Broker, to explain any investigative findings with respect to the nature of the Security Event and the affected Nonpublic Information.

6. **Storage of Nonpublic Information.** Nonpublic Information at rest that is stored, via any method, shall be stored only in data facilities located in the United States that comply with these Security and Privacy Requirements. Unless authorized by Guardian, access to such Nonpublic Information by personnel located outside the United States shall be prohibited. Nonpublic Information will be destroyed by Broker in accordance with any records retention schedules specified by Guardian or Principal.

7. **Return and Destruction of Data.** Upon termination of the Agreement, or upon the request of Guardian or Principal, Broker shall return all Nonpublic Information to Guardian or Principal in a mutually agreed upon, industry standard format, at no cost to Guardian or Principal. For any Nonpublic

Information that Broker does not or cannot return, Broker shall permanently destroy it. Broker may retain Nonpublic Information in electronic format for regulatory and compliance purposes, and in the form of system backups maintained in the ordinary course of business, subject to (i) these Security and Privacy Requirements, including, without limitation, any records retention schedules specified by Guardian or Principal; and (ii) any confidentiality obligations set forth in the Agreement.

8. **Periodic Security Assessment**. Broker shall permit Guardian or Principal to perform (or contract to have performed), at Guardian's expense, a periodic assessment. The assessment will be conducted at a mutually agreed time and will be restricted in scope to cover only those portions of Broker's environment used to access, process or store Nonpublic Information. Broker shall cooperate with Guardian and Principal to determine a plan for correction of any deficiencies, and Broker shall proceed promptly to correct any deficiencies. In the event material deficiencies are found, Guardian or Principal may perform a subsequent security assessment to confirm compliance with these Security and Privacy Requirements.

9. **Cooperation**. Broker shall cooperate with Guardian, Principal and any regulator in connection with the requests or requirements of Guardian, Principal or such regulator including, but not limited to, cooperating in any investigations and responding to any requests from Guardian, Principal or such regulator.

10. **Indemnification**. Broker shall indemnify, defend and hold harmless Guardian and Principal, and Guardian's and Principal's respective affiliates, subsidiaries, parent companies, directors, officers, employees, representatives, contractors, assignees, and successors-in-interest from any losses, claims, liabilities, damages, judgments, fines, and expenses (including attorney's fees and expenses of litigation and settlement) arising out of, connected with, or related to, these Security and Privacy Requirements, which Guardian or Principal may incur or suffer by reason of negligent acts or omissions or willful misconduct of Broker or any vendor or third party used by Broker, material inaccuracy or any misrepresentation or breach by Broker of any term, condition, or warranty contained in these Security and Privacy Requirements.

11. **Confidentiality.** Broker shall not, except as expressly permitted by or required to achieve the purposes of these Security and Privacy Requirements, disclose or use Nonpublic Information or Guardian Data without Guardian's prior written consent. The term "Guardian Data" includes, without limitation, any business strategies, plans, procedures, products, services, proprietary information, software, tools, processes, methodologies, data, and trade secrets of Guardian, and any information of or relating to Guardian's affiliates, employees, clients, customers, agents, suppliers, licensors (including their intellectual property and other proprietary information), and policyholders. Broker shall use Guardian Data only as necessary to perform its obligations in accordance with these Security and Privacy Requirements and not for any other purpose whatsoever, unless other specific uses are requested and authorized in writing by Guardian. Broker may disclose Guardian Data if there is a legal or regulatory requirement to do so, but only to the extent, and only for as long as, and for the limited purposes, as required by law or regulation, provided that Broker, to the extent legally permissible, furnishes prior written notice of such disclosure to Guardian and reasonably cooperates with Guardian, in any effort to seek a protective order or other protection of the Guardian Data. Broker agrees that it will comply with the requirements of all applicable federal and state laws and regulations relating to privacy and treatment of Nonpublic Information.

END OF EXHIBIT A

Exhibit B to Brokerage Agreement Amendment Effective March 1, 2019
Business Associate Agreement for Brokers
LAST UPDATED: 3/15/2019

This Business Associate Agreement ("BAA") for Brokers is incorporated into, and made a part of, the Brokerage Agreement to which you are a party ("Agreement") and can be found on the GuardianLife.com website (the "Site") or via your Principal.

This BAA is made by and between the Broker ("Business Associate") and the Principal ("Principal"). The Guardian Life Company of America, referred to as Guardian, is not a party to this Agreement except to the extent of its endorsement.

Guardian has designated itself as a Hybrid Entity pursuant to 45 CFR § 164.103 and 45 CFR § 164.105 and has identified certain units and departments within Guardian that perform Covered Functions as Health Care Component(s) that are regulated by HIPAA, the HITECH Act, and HIPAA Regulations. For the purpose of this BAA, reference to "Guardian" will also mean the Health Care Component(s) for which the Principal and the Business Associate are providing services. Business Associate and Principal may be referred to individually as a "Party" or collectively as the "Parties."

This BAA may be modified, supplemented or amended at any time and for any reason by Guardian. Any such changes that are posted on the Site from time to time are hereby expressly incorporated herein by reference. We will alert you about any changes by updating the "LAST UPDATED" date (shown above) of this BAA. It is your responsibility to periodically review the Site for any changes to this BAA to stay informed of updates. You will be subject to and will be deemed to have been made aware of, and to have accepted, any changes to this BAA as of the date such revised BAA terms are posted.

In consideration for the promises and the mutual covenants and undertaking set forth in this BAA, Business Associate and Principal agree as follows:

1. Definitions. As used in this BAA:

1.1. "Breach" has the same meaning as this term has in 45 CFR §164.402 and shall include the acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security of privacy of the PHI.

1.2. "Covered Functions" shall have the same meaning as the term "hybrid entity" in 45 CFR §160.103.

1.3. "Designated Record Set" has the same meaning as the term in 45 CFR §164.501 and shall mean a group of records maintained by or for Principal that is (i) the health records and billing records about individuals maintained by or for Principal, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Principal to make decisions about individuals. As used herein, the term "Record" means any item, collection, or grouping of information that includes

Protected Health Information and is maintained, collected, used, or disseminated by or for Principal.

1.4. "Electronic Protected Health Information" or "EPHI" means Protected Health Information supplied by Principal and created, received, transmitted by or maintained in electronic media by either Party.

1.5. "Health Care Component" shall have the same meaning as "health care component" in 45 CFR § 160.103.

1.6. "HIPAA" shall mean the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act, Public Law 104-191, and any amendments thereto.

1.7. "HIPAA Transaction" shall mean Transactions as defined in 45 CFR § 160.103 of the Transaction Standards.

1.8. "HITECH Act" means Subtitle D of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (42 U.S.C. §§ 17921 – 53).

1.9. "Hybrid Entity" shall have the same meaning as the term "hybrid entity" in 45 CFR § 160.103.

1.10. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

1.11. "Law" shall mean all applicable Federal and State statutes and all relevant regulations thereunder, including but not limited to the HITECH Act, and the regulations promulgated thereto (collectively, the "HIPAA Regulations"), which include, as amended from time to time, (i) the privacy standards, requirements and specifications promulgated by the Secretary at 45 CFR Parts 160 and 164 subparts A and E (the "Privacy Rule"), (ii) the security standards, requirements and specifications promulgated by the Secretary at 45 CFR Parts 160 and 164 subparts A and C (the "Security Rule"), (iii) the breach notification standards, requirements and specifications enacted by subtitle D of the HITECH Act and promulgate by the Secretary at 45 CFR. Part 164 subpart D (the "Breach Notification Rule"); and (iv) the HIPAA Enforcement Rule, codified at 45 CFR Part 160, subparts C, D, and E.

1.12. "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information created, received, maintained or transmitted by Business Associate from or on behalf the Health Care Component of Principal.

1.13. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

1.14. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

1.15. "Subcontractor" shall have the same meaning as 45 CFR §160.103 and shall include a person or entity to whom Business Associate delegates a function, activity or service other than in the capacity of a member of the Business Associate's workforce.

1.16. "Transaction Standards" shall mean the Standards for Electronic Transactions, 45 CFR 160 and 162, as they exist now or as they may be amended.

1.17. "Unsecured Protected Health Information" or "Unsecured PHI" shall mean PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in the §13402(h) of the HITECH Act. Unsecured PHI can include information in any form or medium, including electronic, paper or oral.

Terms used, but not otherwise defined, in this BAA (or the Agreement) shall have the same meaning as those terms in the HIPAA Regulations and the HITECH Act.

2. Obligations and Activities of Business Associate.

2.1. Business Associate agrees that it shall not use or further disclose Protected Health Information other than as permitted or required by this BAA or as Required by Law.

2.2. Business Associate shall develop, implement, maintain and use appropriate safeguards to prevent the use or disclosure of Protected Health Information other than as provided for by this BAA.

2.3. Business Associate shall develop, implement, maintain written policies and procedures regarding appropriate administrative, technical and physical safeguards for compliance with the HITECH Act, applicable provisions of the Security Rule and any other applicable implementing regulations issued by the Secretary as they relate to the preservation of the integrity, confidentiality, and availability of electronic Protected Health Information. Business Associate shall ensure that any Subcontractor to whom it provides EPHI agrees in writing to implement reasonable and appropriate safeguards in accordance with requirements of the Security Rule.

2.4. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate or its Subcontractor(s) of a Breach or any other use or disclosure of Protected Health Information in violation of the requirements of this BAA or the HIPAA Regulations.

2.5. Notification Pursuant to an Incident or Breach.

2.5.1. Breach Notification. Business Associate shall promptly, but in no event more than 24 hours following discovery, notify Principal (and Guardian) in writing of any Breach involving Unsecured PHI. Business Associate shall provide an Incident Report (described in Section 2.5.4) of any such Breach of Unsecured Protected Health Information

without unreasonable delay and in any event within five (5) days. Business Associate shall cooperate with Principal (and Guardian) in investigating the breach and in meeting Principal's (and Guardian's) obligations under the breach notification provisions of HIPAA (45 CFR Part 164 Subpart D) and any other applicable Law.

2.5.2. Privacy Incident Notification. With respect to any incident not subject to reporting under the Breach Notification provision of Section 2.5.1 of this BAA, Business Associate shall promptly, but in no event more than 24 hours following discovery, notify Principal (and Guardian) in writing of any other use or disclosure of Protected Health Information of which it becomes aware that is not permitted or required by this BAA. Business Associate shall make such report as soon as administratively feasible and within a timeframe adequate to allow the Principal (and Guardian) to meet its reporting obligation with respect to applicable state and federal reporting requirements or any other applicable Law. Upon Principal's (or Guardian's) request, Business Associate shall promptly provide an Incident Report described in Section 2.5.4 of the Privacy Incident.

2.5.3. Security Incident Notification. With respect to any incident not subject to reporting under Breach Notification and/or Privacy Incident Notification provision(s) of Sections 2.5.1 or 2.5.2 of this BAA, Business Associate shall immediately, but in no event more than 24 hours following discovery, notify Principal (and Guardian) in writing of any successful (a) unauthorized access, use, disclosure, modification, or destruction of Electronic Protected Health Information or (b) unauthorized interference with system operations in Business Associate's information system, of which Business Associate becomes aware. Business Associate shall, upon Principal's (or Guardian's) request, report to Principal (and Guardian) any attempted, but unsuccessful (a) unauthorized access, use, disclosure, modification, or destruction of Electronic Protected Health Information or (b) unauthorized interference with system operations in Business Associate's information systems, of which Business Associate becomes aware. Business Associate shall make such report as soon as administratively feasible and within a timeframe adequate to allow the Principal (and Guardian) to meet its reporting obligation with respect to applicable state and federal reporting requirements or any other applicable Law. Upon Principal's (or Guardian's) request, Business Associate shall promptly provide an Incident Report described in Section 2.5.4 of the Security Incident.

2.5.4. Incident Report Contents. To the extent that any information described below is not available to be included in the Incident Report, the report must include an explanation of why such information is not available to Business Associate. If any such information later becomes available, the information will be provided to Principal (and/or Guardian) as soon as reasonably practicable after it becomes available. Each Incident Report will include the following elements (as applicable):

(i) Identification of each individual whose Protected Health Information is known to have been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during the incident;
(ii) Identification of the nature of the non-permitted access, use, or disclosure and the date of the incident and the date of discovery;

(iii) Identification of the Protected Health Information accessed, used, or disclosed;
(iv) Identification of who made the non-permitted access, use, or received the non-permitted disclosure;
(v) Identification of any corrective action Business Associate has taken or will take to prevent similar Security Incidents in the future;
(vi) Identification of any actions Business Associate has taken or will take to mitigate any harmful effects of the Security Incident;
(vii) An appraisal of whether Business Associate believes its current security measures are adequate given the outcome, scope and nature of the attempt. If existing security measures are not adequate, the Business Associate plans for implementation, which will address the security inadequacies.
(viii) Other such information, as Principal (and/or Guardian) may reasonably request, in meeting the Principal's (and Guardian's) obligations under the breach notification provisions of HIPAA as well as any other applicable Law, including state and/or federal breach notification provisions.

2.5.5. Cooperation; Notification to Affected Individuals and Government Agencies. Business Associate shall cooperate with Principal in any investigation of a Privacy or Security Incident. To the extent Principal (and/or Guardian) determines that a Privacy or Security Incident requires notification or reporting under applicable law or regulation, upon the request and at the sole election of Principal (and Guardian), Business Associate will, on behalf of Principal (and Guardian), prepare and send any or all such notices identified by Principal (and Guardian) to affected individuals and relevant government agencies. To the extent Principal (and Guardian) elects to have Business Associate provide some or all of such notices, Principal (and Guardian) will have the opportunity to review, approve and direct changes to notification(s) and the right to access or receive copies of all communications Business Associate sends or receives in relation to the notifications. Regardless of whether Principal (or Guardian) elects to provide notifications directly, or to have Business Associate provide notifications or its behalf, Business Associate will be responsible for all costs associated with addressing and responding to the notification or reporting obligations, including, but not limited to, costs associated with: (a) investigation of the Privacy or Security Incident (including engaging outside forensics experts, if Principal (or Guardian) deems appropriate); (b) preparing and mailing or other transmission of notifications and other communications to affected Individuals or any other party, as Principal (or Guardian) deems appropriate; (b) establishment of a call center or other communications procedures in response to the Privacy or Security Incident (e.g., Principal (and Guardian) and call center service FAQ's, talking points, and training); (c) public relations and other similar crisis management services; (d) legal and accounting fees and expenses associated with the investigation of and response to the Privacy or Security Incident; (e) costs for providing commercially reasonable credit reporting services that are associated with notifications or have been determined by Principal (and Guardian) as advisable under the circumstances for a period not less than twenty-four (24) months; (f) other costs incurred by Principal (and Guardian) in complying with its legal obligations relating to the Privacy or Security Incident; (g) the cost of providing notice to government agencies, credit bureaus, and/or other required entities; and (h) the cost of any other measures required under applicable Law.

Notwithstanding anything to the contrary in this BAA or any other agreement between the parties, Business Associate's responsibility for these costs are not subject to any contractual monetary limit. This Section shall survive termination of the Agreement and any claim is without regard to any limitation or exclusion of damages or liability provisions otherwise set forth in the Agreement.

2.5.6. Business Associate agrees to ensure that any agent, including a Subcontractor, to whom it provides Protected Health Information agrees in writing to the same restrictions and conditions that apply through this BAA to Business Associate with respect to Protected Health Information, including Electronic Protected Health Information. To the extent that a Subcontractor or other agent of Business Associate creates, receives, maintains or transmits Electronic Protected Health Information on behalf of Business Associate, Business Associate will ensure that the Subcontractor or agent agrees to comply with the applicable requirements of the Security Rule by entering into an agreement that complies with 45 CFR §164.314.

2.5.7. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to Principal, or at the request of Principal to the Secretary, in a time and manner designated by Principal or the Secretary, for purposes of the Secretary determining Principal's (and/or the Business Associate's) compliance with the Privacy Rule and Security Rule.

2.5.8. Business Associate agrees to document disclosures of Protected Health Information, and information related to such disclosures, as would be required for Principal (and/or Guardian) to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528. Business Associate agrees to implement an appropriate record keeping process that will track, at a minimum, the following information: (i) the date of the disclosure; (ii) the name of the entity (or person) who received the Protected Health Information, as well as the address of such entity (or person) if known; (iii) a brief description of the Protected Health Information disclosed; and (iv) a brief statement of the purpose/basis of disclosure (including an explanation).

2.5.9. Business Associate agrees to provide to Principal or an Individual, in a time and manner designated by Principal, information collected in accordance with documentation of disclosure requirements of this BAA (and 45 CFR § 164.528), to permit Principal (and/or Guardian) to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

2.5.10. To the extent reasonably necessary for Principal (and Guardian) to comply with 45 CFR §164.524(c)(2), if Business Associate maintains PHI in an electronic format for any Individual, Business Associate agrees to provide, at the request of an Individual, and in the time and manner designated by the Individual, a copy of such information in the electronic format designated by the Individual to that Individual or, if clearly, conspicuously and specifically directed by the Individual to transmit an electronic copy of that information directly to an entity or person designated by the Individual. If electronic information described in the preceding sentence is not readily producible in the form and format requested by the Individual, it will be provided in a readable electronic form and

format as agreed to by Business Associate and the individual, or, if no agreement is reached in a hard copy format. If a request described in this Section is made by the Individual to Principal (and/or Guardian) instead of Business Associate, Business Associate shall promptly provide Principal with the information in a Designated Record Set as necessary for Principal (and/or Guardian) to comply with an Individual's request for access pursuant to 45 CFR § 164.524.

2.5.11. Upon direction from Principal (and/or Guardian), Business Associate shall amend records in a Designated Record Set as necessary for Principal (and Guardian) to comply with an Individual's amendment request pursuant to 45 CFR § 164.526, or, in the alternative, Business Associate shall allow Principal (and/or Guardian) access to records in a Designated Record Set as necessary for Principal to comply with an Individual's amendment request pursuant to 45 CFR § 164.526.

2.5.12. Business Associate shall comply with any limitation in Guardian's Notice of Privacy Practices (www.guardianlife.com/privacy-policy), as such Notice may be updated from time to time. Business Associate shall comply with any restriction request or confidential communications request to which Principal agrees, provided that Principal (and/or Guardian) makes Business Associate aware of such request.

2.5.13. To the extent that Principal delegates to Business Associate any obligation imposed on Principal by the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Principal in the performance of such delegated obligation.

2.5.14. Business Associate shall encrypt Electronic Protected Health Information prior to saving it on portable media. In any other circumstance, Business Associate shall encrypt Electronic Protected Health Information, including EPHI in transit, unless otherwise agreed upon in writing by Principal.

2.5.15. Upon request, Business Associate shall provide Principal (and/or Guardian) with a list of personnel who are authorized to receive Protected Health Information pursuant to this BAA.

2.5.16. In the event Business Associate receives a subpoena, court or administrative order or other discovery request or mandate for release of Protected Health Information, Business Associate shall notify Principal of the request as soon as reasonably practicable, but in any event within two (2) business days of receipt of such request. Business Associate shall consult Principal prior to its response to a request.

2.5.17. Business Associate, and its agents and subcontractors, if any, are prohibited from directly or indirectly receiving any remuneration in exchange for any of Guardian's PHI.

2.5.18. Business Associate, and its agents and subcontractors, if any, are prohibited from use or disclosure of Genetic Information (as defined in 29 CFR §1635.3(c), except as permitted by 45 CFR § 164.502(a)(5)(i).

3. Permitted Uses and Disclosures by Business Associate.

3.1.General Use. Except as otherwise limited in this BAA, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Principal, provided that such use or disclosure would not violate (i) the Privacy Rule, the HITECH Act or (ii) the minimum necessary as set forth by 45 CFR § 164.502(b) if done by Principal.

3.2.Specific Use and Disclosure.

3.2.1. Except as otherwise limited in this BAA, Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out its legal responsibilities.

3.2.2. Except as otherwise limited in this BAA, Business Associate may disclose Protected Health Information for its proper management and administration, provided that such disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that: (i) it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the entity (or person), and (ii) the person (or entity) will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

3.2.3. Except as otherwise limited in this BAA, Business Associate may use Protected Health Information to provide Data Aggregation services to Principal as permitted by 45 CFR § 164.504(e)(2)(i)(B), to the extent Business Associate performs such services.

3.2.4. Business Associate may use Protected Health Information to report violations of law to appropriate state and/or federal authorities, consistent with 45 CFR § 164.502(j)(1).

4. Obligations of Principal.

4.1. Principal (or Guardian) shall notify Business Associate of any limitation(s) in the Notice of Privacy Practices of Guardian in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information. (Guardian's HIPAA Notice of Privacy Practices may be found at: https://www.guardianlife.com/privacy-policy, and may be subject to change from time to time.)

4.2. Principal (or Guardian) shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

4.3. Principal (or Guardian) shall notify Business Associate of any restriction(s) to the use or disclosure of Protected Health Information that Principal has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction(s) may affect Business Associate's use or disclosure of Protected Health Information.

4.4. Principal shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Principal, except as specifically permissible by this BAA and the Privacy Rule.

5. Termination.

5.1. Termination. This BAA shall terminate upon (i) termination of the Agreement and (ii) when all of the Protected Health Information provided by Principal to Business Associate, or created or received by Business Associate on behalf of Principal, is destroyed, returned or protected in accordance with the terms of this BAA.

5.2. Principal's Termination for Breach. Upon a material breach of the terms of this BAA by Business Associate, Principal shall, at its option: (i) Provide an opportunity for Business Associate to cure the breach or end the violation. Principal may terminate this BAA (and the Agreement) if Business Associate does not cure the breach or end the violation within the time specified by Principal; or (ii) Immediately terminate this BAA (and the Agreement) if Business Associate has breached a material term of this BAA and cure is not possible.

5.3. Other Circumstances Allowing for Immediate Termination. Notwithstanding anything to the contrary in this BAA, Principal may terminate this BAA immediately upon written notice to Business Associate, without any term of notice and/or judicial intervention being required, and without liability for such termination, in the event that Business Associate: (i) is named as a defendant in a criminal proceeding for a violation of any information privacy and protection law; or (ii) is found to have (or stipulates that it has) violated any privacy, security or confidentiality protection requirements under any applicable information privacy and protection law in any administrative or civil proceeding in which Business Associate has been joined.

5.4. Conditions of Termination. Upon termination of this BAA, for any reason, Business Associate shall return to Principal (or destroy) all Protected Health Information. In the event that return (or destruction) of the Protected Health Information is infeasible, Business Associate shall extend the protections of this BAA to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of Business Associate's subcontractors (or agents).

5.5. The termination provisions of this Section 5 shall supersede and replace any contrary provision that may appear in said Agreement.

6. Miscellaneous.

6.1. Amendment. The Parties agree to amend this BAA, as appropriate, to conform to any new or revised legislation, rules and regulations to which Principal is subject now or in the future including, without limitation, the Privacy Rule, Security Rule or Transactions Standards as well as any other applicable state or federal law. Principal may amend this BAA to reflect change to applicable law by providing Business Associate notice of an amendment to this BAA prior to the amendment's effective date, in any manner Principal chooses. Business Associate will be deemed to have agreed to the amendment and the amendment will be binding on Business Associate without signature or other action by Business Associate.

6.2. Assignment. No Party may assign or transfer any or all of its rights and/or obligations under this BAA or any part of it, nor any benefit or interest in or under it, to any third party without the prior written consent of the other Party.

6.3. Survival. The respective rights and obligations of Business Associate under the Conditions of Termination provision shall survive the termination of this BAA.

6.4. Interpretation. Any ambiguity in this BAA shall be resolved to permit Principal (and Guardian) to comply with Law and Transaction Standards.

6.5. Indemnification. Business Associate agrees to indemnify and defend Principal (and Guardian) against and hold it harmless from all claims, damages, losses, judgments, civil monetary penalties, settlements, costs and expenses (including investigation and attorneys' fees) arising out of Business Associate's or its Subcontractor's: (1) negligence or intentional misconduct in the use, disclosure and storage of PHI subject to this BAA; and/or (2) violation of HIPAA, the HITECH Act, HIPAA Regulations or any other federal and/or state health information confidentiality laws and regulations.

6.6. Third Party Rights. The terms of this BAA are not intended, nor should they be construed, to grant any rights to any parties other than Business Associate and Principal.

6.7. Entire Agreement. The BAA constitutes the entire agreement of the Parties with respect to the Parties' compliance with federal and/or state health information confidentiality laws and regulations, as well as the Parties' obligations under the business associate provisions of 45 CFR parts 160 and 164. This BAA supersedes all prior or contemporaneous written or oral memoranda, arrangements, contracts or understandings between the Parties with respect to the Parties' compliance with federal and/or state health information confidentiality laws and regulations.

6.8. Conflict. In the event of a conflict between the terms of the Agreement and this BAA, this BAA will control.

6.9. Electronic Transactions. Business Associate hereby represents and warrants that, to the extent that it is electronically transmitting any of the HIPAA Transactions for Principal, the format and structure of such transmissions shall be in compliance with the Transaction Standards.

6.10. Minimum Necessary. Business Associate shall, if practicable, use, disclose, or request Protected Health Information in a limited data set, as that term is defined in 45 CFR § 164.514(e)(2). Otherwise, Business Associate shall request from Principal or a third party only the minimum amount of information necessary to perform services under this BAA. Business Associate shall develop, implement, maintain and use policies and procedures to limit uses and disclosures of Protected Health Information to the minimum necessary to perform services under this BAA. Business Associate shall determine what constitutes the minimum necessary Protected Health Information to accomplish the intended purpose of any disclosure and shall not solely rely on a request from a third party as being a request for the minimum necessary PHI, except as allowed by the Privacy Rule pursuant to the HITECH Act.

6.11. Notice. Notwithstanding Section 6.1, all notices required under this BAA shall be in writing and shall be deemed to have been given on the next day by fax or other electronic means or upon personal delivery, or in ten (10) days upon delivery in the mail, first class, with postage prepaid. Notices shall be sent to the attention of Guardian's Privacy Office. Either Party may at any time change its address for notification purposes by mailing a notice to the other stating the change and setting forth the new address. Up-to-date information regarding Guardian's Privacy Program may be obtained at: https://www.guardianlife.com/privacy-policy.

6.12. Owner of Protected Health Information. Under no circumstances shall Business Associate be deemed in any respect to be the owner of Guardian's Protected Health Information or any information that is determined to be Guardian's Protected Health Information that may be used or disclosed, created or maintained by or to Business Associate pursuant to the terms of this BAA.

6.13. Irreparable Harm. Business Associate acknowledges and agrees that any use, disclosure or maintenance of any Protected Health Information in a manner inconsistent with this BAA may give rise to irreparable injury to Principal (and Guardian) for which damages would not be an adequate remedy. Accordingly, in addition to any other legal remedies, which may be available at law or in equity, Principal shall be entitled to equitable or injunctive relief against the unauthorized use or disclosure of Protected Health Information or failure to maintain the security of Protected Health Information, as required by this BAA.

END OF EXHIBIT B

Exhibit C to Brokerage Agreement Amendment Effective March 1, 2019
Use of Alternative Group Enrollment Technology Platforms
LAST UPDATED: 3/15/2019

This Exhibit is incorporated into, and made a part of, the Brokerage Agreement to which you are a party ("Agreement") and can be found on the GuardianLife.com website.

Where authorized by a group planholder ("Planholder(s)") of The Guardian Life Insurance Company of America and/or its subsidiaries (collectively, the "Company" or "Guardian"), Broker may perform Administrative Services, as defined in Section 3 below, on Planholder's behalf, utilizing a group benefits administration technology platform ("Platform") as an alternative to using Guardian's proprietary platforms, including *GuardianAnytime*®. This Exhibit sets forth the obligations of Broker when Broker utilizes a Platform to administer a Planholder's Guardian group benefits plan(s) ("Plan(s)"). The term "Platform", as used in this Exhibit, includes Broker's own proprietary Platform, or any Platform utilized by Broker that is owned or operated by a third party service provider(s) ("Third Party Service Provider(s)").

1. Authorization and Notice of Platform Selection. Prior to an RFP/RFQ, Broker shall notify Guardian ("Notification") when a Planholder authorizes Broker to perform Administrative Services utilizing a Platform. Broker represents that it has authority from Planholder to make such Notification. To the extent Broker utilizes a Third Party Service Provider(s) to perform the Administrative Services, the Notification shall also serve as Broker's representation to Guardian and Principal that Planholder has: (i) entered into any necessary agreement(s) with Third Party Service Provider(s), subjecting Third Party Service Provider(s) to security and privacy requirements no less stringent than those set forth in the Agreement, and (ii) authorized Third Party Service Provider(s) to transmit Plan employee, member and dependent (collectively herein referred to as a "Plan Member(s)") information ("Plan Data") to Guardian or its delegate(s). The Notification shall further serve as Broker's representation to Guardian and Principal that the Planholder and/or Broker has obtained all requisite consents from the Plan Members, if required, to transmit Plan Data to Guardian using the Platform. Broker understands that Guardian and Principal will rely on the Notification and all other representations made within this Exhibit, in its dealings with the Planholder, Broker, and Third Party Service Provider(s), if any. Guardian shall at all times have the right to disapprove the use of any Platform.

2. Operational and Service Level Standards. Broker agrees that, in its utilization of a Platform, electronic eligibility and enrollment services provided through the Platform will be accessible to all Plan Members and will facilitate Administrative Services in accordance with the following operational and service level standards:

2.1 Timeliness and Accuracy of Information. Platform shall meet industry standards with respect to the timeliness and accuracy of transmitting Plan Member eligibility and enrollment information to/from Guardian.

2.2 Product Configuration. Platform shall have the capability to configure all Guardian Planholder products to match the appropriate Plan(s) administered, including but not limited to, product offerings, coverage options, member demographic census, and rates.

2.3 In-force Plan Information. Platform shall have the capability to initiate, upload and merge in-force coverage information from Guardian to Platform, when applicable.

2.4 Evidence of Insurability. Platform shall have the capability to initiate the Evidence of Insurability (EOI) process with respect to Guardian's EOI electronic portal (commonly known as "EOI web application") and ensure that the appropriate rules which trigger EOI events are added, when applicable. Platform shall also have the capability to retrieve decisions provided electronically by Guardian and update pending Plan coverage statuses following the completion of the Evidence of Insurability process.

2.5 Electronic Data Interchange. Platform shall have the capability to configure, test, schedule, and initiate the return election file to Guardian (i.e., Electronic Data Interchange (EDI) or other formats) as applicable, consistent with the security and privacy requirements under the Agreement.

2.6 Information Security. Broker and Third Party Service Provider(s) performing Administrative Services shall have a comprehensive information security program that includes administrative, technical and physical safeguards that are appropriate to the nature and scope of the Administrative Services performed, and all Nonpublic Information, as defined under the *Security and Privacy Requirements for Brokers Exhibit* to the Agreement, shall be transmitted in a manner consistent with Guardian's policies and procedures, the terms of the Agreement, and applicable data privacy laws.

2.7 Guardian Plan Data. Guardian Plan Data shall be stored and maintained on a Platform separate and secure from another carrier's data (*e.g.*, medical information shall be segregated from Guardian Plan Data).

2.8 Licensing Requirements. Broker and Third Party Service Provider(s) performing Administrative Services shall be duly licensed, registered or certified to perform the Administrative Services set forth in this Exhibit in all applicable jurisdictions during the term of the Agreement. Broker shall immediately notify Guardian and Principal in the event that any license, registration or certification of Broker or its Third Party Service Provider(s) is revoked or suspended.

2.9 Maintenance Services. Broker and Third Party Service Provider(s) shall maintain the Platform in good working order and condition, so that the Platform will operate in accordance with all applicable standards and requirements set forth in this Exhibit. Furthermore, Broker and Third Party Service Provider(s) shall maintain the Platform and the Administrative Services performed thereon at no additional cost to Guardian or Principal.

2.10 Service Uptime. With the exception of access availability difficulties attributable to:

(i) factors within the exclusive control of Planholder or Plan Member users;
(ii) internet unavailability and other third party telecommunications problems not related to Platform;
(iii) force majeure events; or
(iv) regularly scheduled maintenance of Platform;

Broker and Third Party Service Provider(s) performing Administrative Services shall use commercially reasonable efforts to ensure that the Platform and its functionality are available for Planholder and Plan Members access via the World Wide Web portion of the internet 99.0% of the time.

3. Administrative Services, Broker shall perform either directly, or through Third Party Service Provider(s), the following Administrative Services:

3.1. Electronic Enrollment and Eligibility Maintenance. Electronically enroll and submit electronically updated eligibility information regarding Plan Members as participants in a Plan when they become eligible for participation and in accordance with all applicable Plan provisions and Guardian's policies and procedures. Electronic enrollment and eligibility maintenance shall include promptly coordinating the completion of incomplete information and notifying Guardian electronically of all Plan Member terminations of coverage upon notification by Planholder. Platform enrollment data and documents for all Plan Members shall be maintained in a manner consistent with state insurance records retention laws and regulations.

3.2. Plan Setup and Document Distribution. Timely and accurately conduct Plan set up activities consistent with applicable plan design and deliver applicable Plan documents to Planholders and Plan Members, such as policies, certificates, riders, and other notices consistent with Guardian's policies and procedures and Plan documents, as appropriate.

4. Compliance with Applicable Law. Broker represents that Administrative Services performed under this Exhibit shall at all times comply with all applicable federal and state laws and regulations including, but not limited to, those applicable to licensing, privacy, web content accessibility and those governing the use of electronic signatures. In the event Platform uses electronic signatures, the methodology employed must yield a document that can be authenticated in a court of law in accordance with federal and state evidentiary rules in effect in the jurisdiction where the signature is made.

5. Compensation. Rates of compensation paid by Guardian, if any, to Broker for the performance of Administrative Services shall be set forth in applicable Guardian compensation schedules or as otherwise indicated by Guardian. Any fees paid by Guardian to Broker shall be strictly for the Administrative Services provided for under this Exhibit, and not for any other services provided to Planholder. Additionally, fees shall be no more than the fair market value for the Administrative Services performed.

6. Term. The term of this Exhibit shall continue for as long as the Agreement remains in effect.

7. Plan Transition Services. Upon cancellation or nonrenewal of Plans, or as otherwise requested by Guardian, Broker shall immediately return to Guardian or its designee all Nonpublic Information, stored or accessible on any Platform. The return of Nonpublic Information pursuant to this section shall be executed in a mutually agreed upon manner and in accordance with industry standard format, at no cost to Guardian. For Nonpublic Information that cannot be returned, Broker shall be responsible for permanently destroying such information. Broker may retain Nonpublic Information in electronic format for regulatory and compliance purposes, subject to the information security requirements set forth in the *Business Associate Agreement for Brokers* and *Security and Privacy Requirements for Brokers* Exhibits to the Agreement.

8. Platform Due Diligence. Broker shall permit Guardian to perform, and cooperate with Guardian in performing, due diligence of Platform, including, but not limited to, periodic assessments of Platform's security, privacy and performance of Administrative Services.

9. Errors and Omissions Insurance. While the Agreement is in force and effect, Broker shall maintain Errors and Omissions (E&O) coverage and Network Security and Privacy Liability Insurance coverage in an amount satisfactory to Guardian. Broker shall give Guardian and Principal prompt written notice of any notice of cancellation or change of such coverages.

10. Indemnification. Broker shall defend, indemnify and hold harmless Guardian, Principal and their respective affiliates, parent companies, subsidiaries, directors, officers, employees, representatives, attorneys, vendors, agents, general agents, consultants, clients, customers, and policyholders from all losses, judgments, penalties, damages, costs, and expenses (including reasonable attorney and professional fees) arising out of, connected with, or relating to: (i) Broker's or Third Party Service Provider(s)'s failure to comply with Guardian's security and privacy requirements under the Agreement; (ii) any claims, actions, damages, liabilities, regulatory sanctions, penalties or fines imposed upon Guardian or Principal as a result of acts or omissions of Broker or Third Party Service Provider(s); (iii) any breach by Broker or Third Party Service Provider(s) of any of their respective obligations regarding Nonpublic Information, Guardian data, or security breaches; or (iv) gross negligence or willful misconduct by the Broker or Third Party Service Provider(s).

END OF EXHIBIT C