Guardian

AMENDMENT TO BROKERAGE AGREEMENT – LAST UPDATED: August 15, 2021

This AMENDMENT TO THE BROKERAGE AGREEMENT ("8/15/21 Amendment") is made effective August 15, 2021 (the "Effective Date") by and between The Guardian Life Insurance Company of America and subsidiaries (collectively, the "Company" or "Guardian") and Broker ("Broker"). The Company and Broker are collectively referred to herein as "Parties". This 8/15/21 Amendment can be found on the GuardianLife.com website.

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 Agreement was previously amended effective March 18, 2019 ("3/18/19 Amendment") and the 3/18/19 Amendment was last updated on April 15, 2019; and

WHEREAS, the 3/18/19 Amendment modified the Agreement 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; said security and privacy requirements are reflected in Exhibit A to the 3/18/19 Amendment; and

WHEREAS, said security and privacy requirements have been updated as reflected in this 8/15/21 Amendment, including Exhibit A attached hereto; and

WHEREAS, Exhibit A to this 8/15/21 Amendment replaces Exhibit A to the 3/18/19 Amendment; and

WHEREAS, the Parties agree that this 8/15/21 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 the Security and Privacy Requirements for Brokers (contained in Exhibit A to this 8/15/21 Amendment), which are incorporated into, and made a part of, the Agreement, and which replace Exhibit A to the 3/18/19 Amendment.

3. **Full Force and Effect.** Other than as specifically amended by this 8/15/21 Amendment, the provisions of the Agreement shall remain in full force and effect.

4. **Defined Terms.** Any capitalized terms used in this 8/15/21 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 8/15/21 Amendment and the Agreement, this 8/15/21 Amendment shall prevail.

This 8/15/21 Amendment (including Exhibit A attached hereto) is hereby effectuated by general announcement pursuant to the Amendments section of the Brokerage Agreement. Neither assent nor signature by Broker is required.

Exhibit Attached

Exhibit A – Security and Privacy Requirements for Brokers

Exhibit A

Security and Privacy Requirements for Brokers

LAST UPDATED: August 15, 2021

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"). 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 information, regardless of format, that is not Publicly Available Information (as "Publicly Available Information" is defined by applicable law) and is:

a. Business-related information of Guardian, 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

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, (vi) biometric records, (vii) genetic information or records, (viii) signature, (ix) street address, email address or telephone number, or (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 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, a security breach of Broker's systems and a security breach of any systems of any of Broker's Service Providers.

"Service Provider" means any third party that provides service to Broker and (i) has access to, or that stores or processes, any Nonpublic Information and/or (ii) has access to Guardian's information systems.

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

Without limiting the foregoing, Broker shall adhere to the following minimum requirements as part of its information security program:

- Restrict access to Nonpublic Information to those who have a legitimate business need to access Nonpublic Information for purposes of performing under the Agreement
- Ensure appropriate security awareness training is conducted
- Securely design, develop, install, configure, operate and maintain information systems
- Have a written incident response plan
- Log and monitor access to Nonpublic Information
- Implement secure access control measures, including multifactor authentication for remote access
- Implement encryption at rest and in transit when: (i) required by law or regulation; (ii) as otherwise specified by Guardian; or (iii) as appropriate based on risk.
- Monitor the effectiveness of the information security program (e.g., conducting periodic vulnerability assessments) and make updates as necessary to address risks
- Implement appropriate policies and procedures to assess and manage security risks presented by Service Providers.

3. **Service Provider Requirements.** Broker shall, as part of its information security program, perform appropriate actions, including, but not limited to, overseeing 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 written 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 or any Service Providers are provided with access to any Guardian systems or facilities, Broker shall ensure that any such persons shall comply with (i) all applicable policies and processes of Guardian that Guardian 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 their obligations under the Agreement.

5. **Security Event, Notification and Investigation.** Broker shall immediately, but in no event more than 24 hours, notify 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 shall promptly provide Guardian 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.

7. **Return and Destruction of Nonpublic Information.** Broker shall return all Nonpublic Information in a mutually agreed upon, industry standard format, at no cost to Guardian upon any of the following: (i) termination of the Agreement; (ii) the date on which Nonpublic Information no longer serves a legitimate Guardian business purpose in the performance under this Agreement, which may include, without limitation, the date of removal of Broker as a designated agent/broker of record to a Guardian product or service and date of termination/cancellation of a Guardian product or service as to which Broker is a designated agent/broker of record; or (iii) the written request of Guardian. For any Nonpublic Information that Broker does not or cannot return, Broker shall permanently destroy it in accordance with industry standards to render such information unreadable and unrecoverable and, upon Guardian's written request, provide Guardian with a written certification of such destruction.

   Broker shall be solely and fully responsible for all information not returned or destroyed in accordance with the above requirements, which Broker or its Service Providers possess, maintain, or use for any purpose.

8. **Periodic Security Assessment**. Broker shall permit Guardian 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 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 may perform a subsequent security assessment to confirm compliance with these Security and Privacy Requirements.

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

10. **Indemnification.** Broker shall indemnify, defend and hold harmless Guardian, and Guardian's affiliates, subsidiaries, parent companies, directors, officers, employees, representatives, policyholders, contractors, assignees, predecessors, 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 may incur or suffer by reason of (i) any negligent acts or omissions or willful misconduct of Broker or any Service Provider or (ii) any material inaccuracy or misrepresentation by Broker or any Service Provider or (iii) any breach by Broker or any Service Provider of any term, condition, provision, 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