HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement (this "Agreement") sets forth the agreement between BRIGHTHOUSE LIFE INSURANCE COMPANY and BRIGHTHOUSE LIFE INSURANCE COMPANY OF NY on the one hand ("Brighthouse" or "Covered Entity") and the party identified below as the Business Associate (collectively, the "Parties").

Background

The administrative simplification provisions of HIPAA and related regulations, require that contracts between covered entities and those doing business with a Covered Entity (i.e. Business Associate) comply with enumerated standards and requirements.

The purpose of this Agreement is to confirm that Business Associate comply with the provisions of HIPAA and HITECH. Brighthouse, as an issuer of health insurance products, is a Covered Entity under HIPAA. Brighthouse has appointed Business Associate as a broker to market, sell, and service insurance products ("Services") issued by Brighthouse or one of its affiliates pursuant to a contract between Brighthouse and Business Associate's employer . The Services may involve the use and/or disclosure of Protected Health Information ("PHI"). The Parties acknowledge and agree that in providing Services to Brighthouse, Business Associate will create, receive, use, or disclose PHI. This Agreement addresses the requirements of HIPAA, HITECH, the Privacy Rule, and the Security Rule as they apply to the Business Associate, including the establishment of permitted and required uses and disclosures (and appropriate limitations and conditions on such uses and disclosures) of PHI that is created or received by Business Associate in performing Services on behalf of Covered Entity.

Now therefore, in consideration of the mutual promises below, Brighthouse and Business Associate agree to the following:

1. Definitions

1.01 **General Definitions**. All terms appearing in this Agreement with initial uppercase letters that are not otherwise defined in this Agreement will have the same meaning as that provided for the respective terms in 45 C.F.R. §§ 160.103, 164.103, and 164.501.

1.02 **Breach** means the acquisition, access, use or disclosure of Unsecured Protected Health Information inconsistent with the requirements of Part 164, Subpart E of HIPAA ("Subpart E") which compromises the security or privacy of PHI, unless that acquisition, access, use or disclosure is otherwise excluded under 45 C.F.R. § 164.402. For this purpose, an acquisition, access, use or disclosure of PHI in a manner not permitted under Subpart E is presumed to be a Breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that PHI has been compromised based on a risk assessment.

1.03 **Data Aggregation** shall have the meaning assigned to such a term in 45 CFR § 164.501.

1.04 **Designated Record Set** means a group of records maintained by or for the Covered Entity within the meaning of 45 C.F.R. § 164.501 that consists of: (i) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (ii) records that are used, in whole or in part, by or for the Covered Entity to make decisions about individuals. For purposes of this Section, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Covered Entity.

1.05 **HIPAA** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191.

1.06 **HITECH** means the Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5.

1.07 **Individual** has the same meaning as the term "individual" in 45 C.F.R. § 160.103, and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

1.08 **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.

1.09 **Protected Health Information** means individually identifiable health information that is transmitted by electronic media (within the meaning of 45 C.F.R. § 160.103), maintained in electronic media, or maintained or transmitted in any form or medium including, without limitation, all information (including demographic,

medical, and financial information), data, documentation, and materials that are created or received by Business Associate from or on behalf of the Covered Entity in connection with the performance of Services, and related to:

a. The past, present, or future physical or mental health or condition of an individual;
b. The provision of health care to an individual; or
c. The past, present, or future payment for the provision of health care to an individual.

1.10 **Required By Law** means the same as the term "required by law" in 45 C.F.R. § 164.103.

1.11 **Secretary** means the Secretary of the United States Department of Health and Human Services ("HHS") or his designee.

1.12 **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system as defined in 45 C.F.R. § 164.304.

1.13 **Security Rule** means the Security Standards at 45 C.F.R. Part 160, Part 162 and Part 164.

1.14 **Services** means the functions, activities, or services Business Associate provides or will provide to the Covered Entity under the terms of the Underlying Agreement.

1.15 **Unsecured Protected Health Information** shall have the meaning assigned to such term in 45 CFR § 164.402, limited, however, to the information that Business Associate creates, accesses, or receives on behalf of Covered Entity.

2. Business Associate's Obligations and Activities

2.01 **Non-disclosure of Protected Health Information**. Business Associate agrees not to use or disclose PHI other than as permitted or required by this Agreement or as Required By Law.

2.02 **Safeguards.** Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement and HITECH. Business Associate agrees to implement administrative, physical, and technical safeguards, along with policies and procedures that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information (as defined in HITECH). Business Associate agrees to comply with the applicable standards of 45 CFR § § 164.306, 164.308, 164.310, 164.312, 164.314, and 164.316 with respect to Electronic Protected Health Information.

2.03 **Mitigation.** Business Associate agrees to mitigate, to the extent practicable, any harmful effects known to Business Associate about the use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement, the Privacy Rule, the Security Rule, or other applicable federal or state laws concerning the privacy or security of PHI. Business Associate shall promptly thereafter provide Brighthouse with a written report of such harmful effects and related issues and corresponding actions taken by Business Associate.

2.04 **Reporting of Violations.** Subject to Section 2.05, Business Associate agrees to report to Brighthouse any impermissible use or disclosure of PHI not permitted by this Agreement within 5 business days of the impermissible use or disclosure or Business Associate's discovery of the impermissible use or disclosure. For purposes of this Section, an impermissible use or disclosure is treated as discovered as of the first day on which the impermissible use or disclosure is known to the Business Associate, or, by exercising reasonable diligence would have been known to the Business Associate, consistent with 45 C.F.R. § 164.404. Business Associate shall also report to Brighthouse any Security Incident of which Business Associate becomes aware within 48 hours.

2.05 **Breach of Protected Health Information.** Following discovery of a Breach or impermissible disclosure of Unsecured Protected Health Information, the Business Associate is required to identify the individual(s) whose PHI has been acquired, accessed, used, or disclosed and to notify Brighthouse without unreasonable delay, but no later than 48 hours after discovery of the Breach. For purposes of this Section, a Breach is treated as discovered as of the first day on which such Breach is known to the Business Associate, or, by exercising reasonable diligence would have been known to the Business Associate consistent with 45 C.F.R. § 164.404. Upon discovering the Breach, the Business Associate is also required to:

a. Identify the entity to which the information was impermissibly disclosed;

b. Determine, to the best of its knowledge based on the information of which it becomes aware during its investigation, whether or not the entity is subject to HIPAA and the Privacy Rule;
c. Identify the type and amount of PHI disclosed;
d. Perform a risk assessment as described pursuant to the definition of "Breach" under 45 C.F.R. § 164.402 to determine whether the Business Associate believes there is a low probability that the PHI has been compromised;
e. If the improperly disclosed PHI is returned, determine if the information was returned before being accessed for an improper purpose; and
f. Provide Brighthouse with a written report of the information described above without unreasonable delay.

2.06 Notice of a Breach of Protected Health Information. In the event of a Breach, the Business Associate, with prior written approval of Brighthouse, will notify the affected individuals without unreasonable delay, but no later than 30 days after discovery of the Breach ("Notice Date"). The notice will include the information required under 45 C.F.R. § 164.404(c), including but not limited to:

a. a brief description of the Breach;
b. date the Breach occurred;
c. date the Breach was discovered, if known;
d. type of PHI involved;
e. steps that the individual should take to protect him/herself from potential harm resulting from the Breach;
f. brief description of steps Business Associate has taken to investigate, mitigate losses, and protect against further Breaches; and
g. contact information for individuals to ask questions, including a toll-free number, e-mail address, website, or postal address.

To the extent that the Breach involves more than 500 residents of a single state or jurisdiction, Business Associate must provide Brighthouse, no later than the Notice Date, the information necessary for Covered Entity to prepare a notice to media outlets as set forth in 45 C.F.R. § 164.406. To the extent that the Breach involves more than 500 Individuals, Business Associate must provide Brighthouse, no later than the Notice Date, the information necessary for Covered Entity to prepare a notice to the Secretary as set forth in 45 C.F.R. § 164.408. To the extent that the Breach involves 500 individuals or fewer, Business Associate must maintain a log of those Breaches ("Breach Log") and provide that log to Brighthouse for submission to HHS. Business Associate will provide the Breach Log to Brighthouse annually, not later than 30 days after the end of the calendar year.

2.07. Audits. Business Associate will allow Brighthouse to audit Business Associate's compliance with the Privacy Rule, Security Rule and this Agreement upon prior notice.

2.08. Agents and Subcontractors. Business Associate agrees to ensure that any Business Associate agent or subcontractor (as defined in 45 CFR § 160.103), including the Business Associate's Affiliates, that creates, receives, maintains or transmits PHI on its behalf agrees in writing to terms and conditions substantially similar to those that apply to Business Associate with respect to such PHI under this Agreement.

2.09. Independent Entities. This Agreement shall establish no relationship between the Parties other than that of independent contractors. Neither Brighthouse nor Business Associate, nor any of their respective Subcontractors, agents or employees, shall be construed to be the agent, employee or representative of the other. None of the provisions of the Agreement are intended to create, nor shall they be deemed or construed to create, any partnership, joint venture, or other relationship between the Parties except that of independent contracting entities. Business Associate acknowledges that it has independent obligations to comply with certain requirements under HIPAA. Brighthouse does not make any warranties, representations or guarantees that this Agreement satisfies Business Associate's independent obligations to comply with HIPAA.

2.10. Sanctions. If Business Associate becomes aware of a pattern of activity or practice of its agents or Subcontractors that constitutes a material violation of the obligations under Section 2.08, or Brighthouse's privacy policies and procedures, Business Associate agrees to take reasonable steps to cure or end the violation, and if such steps are unsuccessful, to terminate its agreement with the agent or subcontractor, if feasible.

2.11. Amendment of Protected Health Information. Business Associate agrees to make appropriate amendments to PHI in a Designated Record Set that either Covered Entity, or an Individual, requests pursuant to procedures established under 45 C.F.R. § 164.526. To the extent Business Associate receives a request by an Individual to amend his or her PHI, Business Associate will communicate its approval or denial of any such request by following mutually agreed upon procedures.

2.12. **Disclosure of Internal Practices, Books, and Records.** Business Associate agrees to make its internal practices, books and records (including policies and procedures) about the use and disclosure of PHI received from or created by Business Associate on behalf of Covered Entity available to Brighthouse without unreasonable delay or, at Brighthouse's request, to the Secretary, in a time and manner designated by Brighthouse or the Secretary.

2.13. **Access to Protected Health Information.** Business Associate agrees promptly to notify Brighthouse of an Individual's request to inspect or get a copy of his or her PHI (as provided for in 45 C.F.R. § 164.524) in Business Associate's possession or in a Designated Record Set and agrees to respond to such requests within 30 days of receipt as long as complying with that request would not violate HIPAA or the Privacy Rule. If Brighthouse submits a request to Business Associate for access to PHI in a Designated Record Set, Business Associate agrees to provide access such PHI as directed in writing by Brighthouse, in accordance with the requirements of 45 CFR §§ 164.524.

2.14. **Documentation of Disclosures.** Business Associate agrees to document disclosures of PHI and information about disclosures as would be required for a Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI consistent with 45 C.F.R. § 164.528. At a minimum, this documentation will include:

a. Date of each disclosure;
b. Name of the entity or person who received PHI and, if known, the address of the entity or person;
c. Brief description of the PHI disclosed;
d. Subject to Section 2.15, the disclosures of PHI, if any, that occurred during the six-year period prior to the date of the request for an accounting (or any shorter period of time requested by the Individual), and that are otherwise subject to the accounting requirement in 45 C.F.R. § 164.528; and
e. Brief statement explaining to the Individual why the disclosure was made or, if applicable, instead of this statement, a copy of the written request that formed the basis for the disclosure.

2.15. **Accounting for Disclosures.** Business Associate agrees to provide Brighthouse or an Individual information collected in accordance with Section 2.14 in a timely manner mutually agreed upon to enable Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI consistent with 45 C.F.R. § 164.528.

2.16. **Facilitate the Exercise of Privacy Rights.** Business Associate agrees to establish procedures that allow Individuals to exercise their rights under the Privacy Rule, including the right to:

a. Inspect and obtain copies of records and documents within the possession or control of the Business Associate that contain the Individual's PHI;
b. Request amendments to their PHI;
c. Receive an accounting of disclosures Business Associate made of their PHI
d. Request restrictions on the use or disclosure of their PHI; and
e. Receive communications regarding their PHI at alternative locations or by alternative means.

2.17. **No Waiver of Rights.** Business Associate agrees not to require Individuals to waive their health information privacy rights as a condition for treatment, payment, or eligibility for health benefits.

2.18. **Responses to Subpoenas.** If Business Associate receives a subpoena, discovery request or other lawful process, with or without an order from a court or administrative tribunal, relating to Brighthouse, the Covered Entity or this Agreement, including any use or disclosure of PHI or any failure in Business Associate's health data security measures, Business Associate agrees to fully comply with the notice and protective action obligations set forth in 45 C.F.R. § 164.512(e), the requirements of Section 3.04 (below), and Business Associate's policies and procedures regarding subpoenas, discovery requests and other lawful process, which policies and procedures will be communicated to Brighthouse upon request. Without limiting the foregoing, Business Associate shall notify Brighthouse within five (5) business days of the Business Associate's receipt of any request or subpoena for PHI. Brighthouse shall have the right to assume responsibility for challenging the validity of such request, in which case Business Associate shall fully cooperate with Brighthouse in such a challenge.

2.19. **Electronic Transactions.** To the extent required by HIPAA (including the Standards for Electronic Transactions at 45 C.F.R. Parts 160 and 162), Business Associate agrees to use or conduct, in whole or in part, standard transactions and use code sets or identifiers under the Privacy Rule for Brighthouse or on behalf of Covered Entity as detailed under the Privacy Rule or HIPAA. Business Associate will also require its agents and Subcontractors to comply with these electronic transaction requirements under HIPAA.

2.20. **Security Standards.** Business Associate acknowledges that it may need to issue and change procedures from time to time to improve electronic data and file security, and agrees that those measures will be at least as stringent as may be required by the Privacy Rule, the Security Rule, or other federal, state and local laws, rules and regulations concerning the privacy and security of PHI, as applicable.

2.21. **Notice of Privacy Practices.** Covered Entity will prepare and distribute a notice of privacy practices as required by the Privacy Rule. If Business Associate maintains a website on behalf of Covered Entity that provides information about the Covered Entity's services or benefits, Business Associate will make the notice of privacy practices available electronically through the website, and will make certain that the notice of privacy practices is prominently posted on the website.

2.22. **Compliance with Laws.** Business Associate shall comply with all applicable federal, state and local laws, rules and regulations concerning the privacy and security of PHI, including, without limitation, the requirements of HIPAA, the HITECH, and Genetic Information Nondiscrimination Act of 2008 ("GINA").

3. Business Associate's Permitted Uses and Disclosures

3.01. **General Uses and Disclosures.** Business Associate agrees to create, receive, use or disclose PHI only in a manner that is consistent with this Agreement, the Privacy Rule and the Security Rule, and only for the purposes of providing services to Brighthouse on behalf of the Covered Entity, as Required By Law, or as expressly permitted in this Agreement. Business Associate will limit its disclosure of PHI to the minimum necessary to accomplish the intended purpose of such disclosure. Business Associate will not use or disclose PHI in any manner that would constitute a violation of 45 C.F.R. Parts 160 and 164.

3.02. **Use for Management and Administration of Business Associate.** In accordance with 45 C.F.R. § 164.504(e)(4)(i), Business Associate may use PHI to carry out its legal responsibilities and for its proper management and administration.

3.03. **Disclosure for Management and Administration of Business Associate.** Business Associate may, with Brighthouse's prior written approval, disclose PHI to carry out its legal responsibilities or for its proper management and administration if the disclosure is (1) Required by Law; or (2) the Business Associate obtains reasonable assurances from the person to whom the information is to be disclosed that the:

a. Information will remain confidential;
b. Information will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person; and
c. Person will notify the Business Associate if the confidentiality of the information is breached.

3.04. **Uses and Disclosures Required by Law.** Business Associate may use and disclose PHI to the extent such use or disclosure is Required By Law provided (a) the use or disclosure complies with and is limited to the relevant requirements of such law, (b) Business Associate promptly notifies Brighthouse of such use or disclosure and, at Brighthouse's request and Business Associate's expense, assists in obtaining a protective order or other similar order, and (c) the use or disclosure complies with the requirements of 45 CFR § 164.512 to the same extent such requirements would apply if the use or disclosure were made by Covered Entity.

3.05. **Use of Data Aggregation Services.** Business Associate may use PHI to provide Data Aggregation services to Brighthouse about the Covered Entity's health care operations as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

3.06. **Prohibition on Sale of Protected Health Information.** Except as permitted under 45 CFR § 164.502(a)(5)(ii), Business Associate agrees not to directly or indirectly receive remuneration in exchange for any PHI of any Individual.

4. Term and Termination

4.01 In addition to any other termination rights available to the Parties, upon Brighthouse's knowledge of a material violation by Business Associate of this Agreement, Brighthouse may: (i) immediately terminate this Agreement and de-appoint the Business Associate if Business Associate has violated a material term of this Agreement and cure is not possible; or (ii) terminate this Agreement and the Underlying Agreement upon 30 days' notice if Brighthouse determines that Business Associate has violated a material term of this Agreement and if, following Brighthouse's notification to Business Associate of the material violation, Business Associate is

unable or unwilling to take steps to cure the violation within such 30 day period. In the event of such a cure, this Agreement shall remain in full force and effect.

4.02 Upon termination of this Agreement, Business Associate will destroy or return all PHI provided by Brighthouse to the Business Associate or created or received by Business Associate on behalf of Brighthouse. If it is infeasible to return or destroy PHI, Business Associate will extend the protections afforded to PHI by this Agreement to that PHI indefinitely and such obligations shall survive the termination of this Agreement.

5. Miscellaneous

5.1 **Amendments.** The Parties agree to take the necessary action to amend this Agreement from time to time to allow Brighthouse to comply with changes to the requirements of the Privacy Rule, Security Rule, HIPAA, or other federal, state and local laws, rules and regulations, as applicable.

5.2 **Interpretation.** Any ambiguity in this Agreement will be resolved in favor of a meaning that permits Brighthouse to comply with the Privacy Rule or the Security Rule, as applicable.

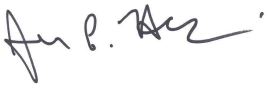
5.3 **Inconsistency.** A court or regulatory agency with authority over the Parties will resolve any inconsistencies between the provisions of this Agreement and the Privacy Rule or Security Rule, as may be amended from time to time, in favor of the Privacy Rule or Security Rule. The provisions of this Agreement will control, however, for any provisions in this Agreement that are not the same as, but are nonetheless permitted by, the Privacy Rule or Security Rule.

5.4 **Amendment of Plan Documents.** To the extent Business Associate performs plan administration functions for a group health plan, as defined by 45 CFR § 160.103, Business Associate represents that the Plan Sponsor has amended the Plan documents and signed a certification for the Plan in accordance with the Privacy Rule requirements at 45 C.F.R. § 164.504(f) relating to disclosure of PHI to the Plan Sponsor for certain plan administration functions, and that Plan Sponsor will only use and disclose PHI in accordance with those Plan document provisions.

5.5 **Underlying Agreement.** Except as specifically required to implement the purposes of this Agreement, to the extent inconsistent with this Agreement, all terms of the Underlying Agreement shall remain in full force and effect. In the event of a conflict between the terms of the Underlying Agreement and this Agreement, this Agreement shall control.

5.6 **Survival.** The terms of Section 2.03, 2.04, 2.05, Section 2.12, Section 2.15, Section 5, and Section 5.06 shall survive the termination or expiration of this Agreement.

5.7 **Indemnification.** Business Associate agrees to indemnify, defend, and hold harmless Brighthouse and its directors, officers, affiliates, employees, agents, subcontractors and successors from and against any and all claims, losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or related to Business Associate's violation of its obligations under this Agreement.

Brighthouse Life Insurance Company **Brighthouse Life Insurance Company of NY Signature**: 	**Business Associate** **Signature:**
Printed Name: Jeffrey P. Halperin **Title:** Chief Compliance Officer & Associate General Counsel **Date: August 17, 2021**	**Printed Name:** **Title:** **Date:**