

NYL – BUSINESS ASSOCIATE AGREEMENT

The following Business Associate Agreement (“**BAA**”) supplements or modifies the terms and conditions of the Agreement with respect to the provision of products, goods and services by Supplier that require access to or use of PHI. In the event of any conflict or inconsistency between this BAA and the Agreement, this BAA will take precedence in interpretation with respect to their subject matter.

1. DEFINITIONS.

- (A) “**Agreement**” means any written contract, agreement, or order entered into by NYL and Supplier for the procurement of products, goods, and services. Agreements include, without limitation, (i) framework/master/governing agreements, (ii) orders made to a framework/master/governing agreement, (iii) single-use or stand-alone agreements, and (iv) purchase orders, direct to source orders, or any similar type of ordering documents.
- (B) “**Applicable Law**” means, as applicable to NYL and Supplier (directly and as service providers to NYL), or the subject matter of this BAA or the Agreement, for all countries, all then-current national, federal, state, provincial, or local: (i) laws (including common law), ordinances, regulations, and codes; (ii) the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA); (iii) binding court orders, judgments, or decrees (including consent agreements); (iv) regulatory orders, requirements, directives, policies, rules, decisions, judgments, interpretive letters, guidance, and other official releases; and (v) anti-corruption laws including the U.K. Bribery Act and the U.S. Foreign Corrupt Practices Act.
- (C) “**HIPAA Rules**” means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.
- (D) “**NYL**” means New York Life Insurance Company, its affiliates, and their respective personnel.
- (E) “**Personal Data**” means any data or information, that, either individually or when combined with other information, could be used to distinguish or trace an individual’s identity, including (i) information about or related to natural persons that is explicitly defined as a regulated category of data or given protected status under Applicable Law; (ii) non-public information, such as a government-issued passport, Social Security, driver’s license, or other identification number, (iii) PHI and other health or medical information, such as insurance, medical, diagnosis, genetic, or biometric records or information; (iv) financial and insurance information, such as employee compensation or a policy, credit card, or bank account number; or (v) sensitive personal data, such as name, address, telephone number, date and place of birth, mother’s maiden name, race, marital status, gender, information regarding an individual’s education, criminal history, employment history or sexuality).
- (F) “**Protected Health Information**” or “**PHI**” means, as defined at 45 C.F.R. §160.103 or any successor provision, information that (i) is received from, or created and received on behalf of, NYL, (ii) identifies (or can reasonably be used to identify) an individual (whether living or deceased), and (iii) relates to the past, present, or future physical or mental health or condition of that individual, the provision of health care to that individual, or the past, present, or future payment for the provision of health care to that individual.
- (G) “**Security Incident**” means any actual, alleged, or suspected unauthorized or inadvertent access, disclosure, improper handling, compromise, or theft of NYL’s confidential information, NYL systems, Personal Data, NYL materials, or Supplier’s systems.
- (H) “**Supplier**” means, for the general purposes of this BAA, an entity (including its affiliates, contractors, service providers, and personnel) that has entered into an Agreement with NYL for the provisions of products, goods and services.

- 1.2 Alignment to Rules.** For purposes of this Exhibit, the following terms have the same meaning as given in the HIPAA Rules: Breach, Individual, Required By Law, and Security Incident.
- 2. DUTY OF CARE.** With respect to any PHI that forms a part of NYL Confidential Information (as defined in the Agreement), and in addition to its obligations under the Agreement with respect to confidentiality, Supplier will further ensure that use and disclosure of PHI is in accordance with the HIPAA Rules and the applicable provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act provisions of the American Recovery and Reinvestment Act of 2009, Pub. Law No. 111-5, and its implementing regulations.
- 3. USE RESTRICTIONS.** In addition to any restrictions with respect to use and disclosure of NYL Confidential Information in the Agreement, as relates to PHI, Supplier will not use or disclose PHI in any manner that would constitute a violation of 45 C.F.R. Parts 160 and 164 if PHI was so used or disclosed by NYL in this same manner, and will only permit access to PHI to Supplier personnel on a strict need to know basis and then only as required for Supplier to provide the products, goods and services.
- 4. SECURITY REQUIREMENTS.** Supplier will comply with the security requirements for electronic PHI as set forth in the applicable provisions of the HIPAA Rules including, but not limited to, 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316 if these security requirements are more robust, rigorous, and stringent than those identified in this Agreement.
- 5. SECURITY INCIDENT REPORTING.**
- 5.1 Reporting Security Incidents.** In addition to Supplier's obligations under the Agreement with respect to reporting of a Security Incident, Supplier will ensure it complies with all requirements required by 45 C.F.R. 164.410 with respect to the actual or suspected loss of PHI.
- 5.2 Obligations.** Further, for any Security Incident involving PHI, Supplier will:
- (A) Information.** Include in its incident report a thorough description of the Breach or Security Incident, the name(s) of the affected Individual(s), the date of the Breach or Security Incident, including the date of the discovery of the Breach or Security Incident, type(s) of PHI impermissibly accessed or disclosed and, if the PHI was computerized data, whether the PHI was encrypted or protected by any other method or technology that renders the electronic files, media, or databases unreadable or unusable, and such other information that NYL may request;
 - (B) Cooperation.** Cooperate fully with NYL with the investigation and handling of any Breach or Security Incident, including the notification to affected Individuals, consumer reporting agencies, and, if Required By Law, all applicable Regulators. Supplier agrees to cooperate with NYL with the remediation of Individuals who may have been adversely affected by a Breach or Security Incident involving PHI that Supplier collects, uses, discloses, or maintains on NYL's behalf as part of these Supplier Functions. Supplier will be fully responsible for any Breach or Security Incident and all costs or expenses for any notification and/or remediation of Individuals affected; and
 - (C) Remediation.** Employ measures to promptly remedy the Breach or Security Incident and protect against future occurrences.
- 6. INDIVIDUAL ACCESS.** Within 15 business days after NYL's request, Supplier will accommodate an Individual's access to his or her PHI in a manner consistent with the HIPAA Rules. If an Individual contacts Supplier directly about access to PHI, Supplier will not provide access to the Individual but will forward such request to NYL within three business days after such contact.
- 7. AMENDMENTS TO PHI.** Within 15 business days after NYL's request, Supplier will make all necessary amendments to PHI in a manner consistent with the HIPAA Rules. If an Individual contacts

Supplier directly about making amendments to PHI, Supplier will not make any amendments to the Individual's PHI but will forward such request to NYL within three business days after such contact.

8. RECORDKEEPING. In addition to any other recordkeeping requirements mandated by Applicable Law, Policies, the Agreement, or this BAA:

8.1 Regulatory Access. Supplier will make its internal practices, books and records relating to uses and disclosures of PHI available to NYL or to Regulators for purposes of determining NYL's and Supplier's compliance with the HIPAA Rules.

8.2 Permitted Disclosures. Supplier will keep a record of disclosures of PHI and agrees to make information regarding disclosures of PHI available to NYL within 15 business days after NYL's request, in a manner consistent with the HIPAA Rules. Supplier will provide, at a minimum, the following information: (A) the date of disclosure; (B) the name of the entity or person who received the PHI, and the address of such entity or person, if known; (C) a brief description of the PHI disclosed; (D) a brief statement regarding the purpose and explanation of the basis of such disclosure and (E) the names of all Individuals whose PHI was disclosed.

9. RESTRICTIONS. Supplier will comply with any other restrictions on the use or disclosure of PHI that NYL has adopted or is required to abide by under the HIPAA Rules, to the extent that such restriction may affect Supplier's use or disclosure of PHI.

10. AMENDMENTS. The Parties agree to take such action as is necessary to amend the Agreement and this BAA as is necessary for compliance with the requirements of the HIPAA Rules and any other Applicable Law.