Benelinx
Business Associate Agreement

This Business Associate Agreement (this **"BAA"**) is entered into by and between Benelinx, LLC, a Colorado limited liability company (**"Provider"** or **"Business Associate"**), and the customer identified on the applicable Order Form (**"Customer"** or **"Covered Entity"**). Provider and Customer are each a **"Party"** and together the **"Parties."**

This BAA supplements and forms part of the Benelinx Terms of Service between Customer and Provider (the **"Agreement"**). Capitalized terms used but not defined in this BAA have the meanings given to them in the Agreement. In the event of a conflict between this BAA and the Agreement with respect to the use, disclosure, or protection of PHI (as defined below), this BAA shall control.

RECITALS

WHEREAS, Customer may be a Covered Entity or a Business Associate (as those terms are defined under HIPAA) that creates, receives, maintains, or transmits Protected Health Information in connection with its business operations;

WHEREAS, Provider operates a cloud-based software-as-a-service platform (the "**Service Platform**") built on the Salesforce ecosystem that enables Customer to manage employee benefits agency operations, which may involve the receipt, maintenance, transmission, or creation of Protected Health Information on behalf of or at the direction of Customer;

WHEREAS, the Parties desire to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act ("**HITECH Act**"), and the regulations promulgated thereunder at 45 C.F.R. Parts 160 and 164 (collectively, "**HIPAA**" or the "**HIPAA Rules**"), and to establish the terms under which Provider will safeguard PHI;

NOW, THEREFORE, in consideration of the mutual promises set forth herein and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. DEFINITIONS

The following terms shall have the meanings set forth below. Any capitalized terms used in this BAA that are not defined herein shall have the meanings ascribed to them in the HIPAA Rules or the Agreement, as applicable.

1.1 **"Breach"** has the meaning set forth in 45 C.F.R. § 164.402.

1.2 **"Covered Entity"** shall generally have the meaning set forth in 45 C.F.R. § 160.103, and as used in this BAA refers to Customer, whether Customer is itself a Covered Entity or a Business Associate acting on behalf of a Covered Entity. Where Customer is a Business Associate of a third-party Covered Entity, references to "Covered Entity" in this BAA shall be interpreted to impose equivalent obligations on Provider as a subcontractor under HIPAA.

1.3 **"Designated Record Set"** has the meaning set forth in 45 C.F.R. § 164.501.

1.4 **"Disclosure"** has the meaning set forth in 45 C.F.R. § 160.103.

1.5 **"Electronic Protected Health Information" or "ePHI"** has the meaning set forth in 45 C.F.R. § 160.103.

1.6 **"HIPAA Rules"** means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164.

1.7 **"Individual"** has the meaning set forth in 45 C.F.R. § 160.103 and includes a person who qualifies as a personal representative under 45 C.F.R. § 164.502(g).

1.8 **"Protected Health Information" or "PHI"** has the meaning set forth in 45 C.F.R. § 160.103, limited to the information created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity pursuant to the Agreement.

1.9 **"Required by Law"** has the meaning set forth in 45 C.F.R. § 164.103.

1.10 **"Secretary"** means the Secretary of the U.S. Department of Health and Human Services or the Secretary's designee.

1.11 **"Security Incident"** has the meaning set forth in 45 C.F.R. § 164.304.

1.12 **"Subcontractor"** has the meaning set forth in 45 C.F.R. § 160.103.

1.13 **"Unsecured Protected Health Information"** has the meaning set forth in 45 C.F.R. § 164.402.

1.14 **"Use"** has the meaning set forth in 45 C.F.R. § 160.103.

1.15 **Regulatory References.** A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.

2. OBLIGATIONS OF BUSINESS ASSOCIATE

2.1 **Permitted Uses and Disclosures.** Business Associate shall not Use or Disclose PHI other than as permitted or required by this BAA, the Agreement, or as Required by Law. Business Associate is permitted to Use and Disclose PHI as necessary to perform its obligations under the Agreement, including to provide the Service Platform and related Support Services and Professional Services, subject to the restrictions in this BAA.

2.2 **Minimum Necessary Standard.** To the extent required by the HIPAA Rules, Business Associate shall limit its Use, Disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose of such Use, Disclosure, or request.

2.3 **Safeguards.** Business Associate shall implement and maintain appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits on behalf of Covered Entity, as required by the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C). Business Associate shall comply with the requirements of the HIPAA Security Rule applicable to business associates, including 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316. Customer acknowledges that the Service Platform operates on the Salesforce platform ("SFDC Platform"), and that certain infrastructure-level security controls (including physical data center security, network-level encryption, and platform-level access controls) are maintained by Salesforce. Business Associate does not independently warrant or guarantee the security measures of Salesforce but shall maintain its own application-level safeguards and shall use commercially reasonable efforts to select and utilize infrastructure providers that maintain appropriate security certifications and practices.

2.4 **Reporting.**

(a) Business Associate shall report to Covered Entity any Use or Disclosure of PHI not provided for by this BAA of which Business Associate becomes aware, including any Breach of Unsecured Protected Health Information as required by 45 C.F.R. § 164.410.

(b) Business Associate shall report to Covered Entity any Security Incident of which Business Associate becomes aware. For purposes of this provision, the Parties acknowledge that unsuccessful attempts at unauthorized access to ePHI (such as pings, port scans, unsuccessful log-on attempts, or denial-of-service attacks) occur routinely and do not constitute reportable Security Incidents. Business Associate's obligation to report Security Incidents is limited to events that

result in actual unauthorized access, Use, Disclosure, modification, or destruction of ePHI, or interference with Business Associate's system operations that materially compromise ePHI.

2.5 **Breach Notification.** Business Associate shall notify Covered Entity without unreasonable delay, and in no event later than seventy-two (72) hours after confirming a Breach of Unsecured Protected Health Information. The notification shall include, to the extent reasonably available at the time of notification: (a) identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed during the Breach; (b) a brief description of what happened, including the date of the Breach and the date of discovery; (c) a description of the types of Unsecured Protected Health Information involved; (d) any steps Individuals should take to protect themselves from potential harm; and (e) a description of what Business Associate is doing to investigate, mitigate, and prevent future occurrences. If complete information is not available at the time of initial notification, Business Associate shall provide such information in supplemental notifications as it becomes available. Business Associate shall cooperate with Covered Entity's investigation, mitigation, and notification efforts.

2.6 **Subcontractors.** In accordance with 45 C.F.R. § 164.502(e)(1)(ii) and § 164.308(b)(2), Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees to the same restrictions, conditions, and requirements that apply to Business Associate under this BAA with respect to such PHI. Business Associate shall enter into a written agreement with each such Subcontractor that contains terms no less restrictive than this BAA. For the avoidance of doubt, the SFDC Platform (Salesforce) is a Subcontractor under this BAA, and Business Associate represents that it has entered into appropriate agreements with Salesforce that address the protection of PHI.

2.7 **Access to PHI.** To the extent Business Associate maintains PHI in a Designated Record Set on behalf of Covered Entity, Business Associate shall, within ten (10) business days of a written request from Covered Entity, make available to Covered Entity such PHI as necessary for Covered Entity to satisfy its obligations under 45 C.F.R. § 164.524. If Business Associate receives a request for access to PHI directly from an Individual, Business Associate shall promptly forward such request to Covered Entity.

2.8 **Amendment of PHI.** To the extent Business Associate maintains PHI in a Designated Record Set on behalf of Covered Entity, Business Associate shall, within ten (10) business days of a written request from Covered Entity, make any amendment(s) to PHI as directed by Covered Entity pursuant to 45 C.F.R. § 164.526. If Business Associate receives a request for amendment directly from an Individual, Business Associate shall promptly forward such request to Covered Entity.

2.9 **Accounting of Disclosures.** Business Associate shall maintain an accounting of Disclosures of PHI as would be required for Covered Entity to respond to a request by an Individual under 45 C.F.R. § 164.528. Business Associate shall, within fifteen (15) business days of a written request from Covered Entity, make available to Covered Entity the information required to provide an accounting of Disclosures. At a minimum, such information shall include: (a) the date of each Disclosure; (b) the name and, if known, the address of the entity or person who received the PHI; (c) a brief description of the PHI disclosed; and (d) a brief statement of the purpose of the Disclosure or a copy of the request for Disclosure.

2.10 **Availability to HHS.** Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received on behalf of, Covered Entity available to the Secretary for purposes of determining Covered Entity's or Business Associate's compliance with the HIPAA Rules, subject to applicable legal privileges.

2.11 **Prohibition on Sale of PHI.** Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except as permitted under 45 C.F.R. § 164.502(a)(5)(ii).

2.12 **Restrictions on Marketing and Fundraising.** Business Associate shall not Use or Disclose PHI for marketing or fundraising purposes unless expressly authorized in writing by Covered Entity and consistent with 45 C.F.R. §§ 164.501, 164.508, and 164.514(f).

2.13 **De-identification.** Business Associate may de-identify PHI in accordance with 45 C.F.R. § 164.514(a)-(c) for lawful purposes, provided that de-identification is performed using methods that satisfy the requirements of the HIPAA Rules and that de-identified data cannot reasonably be used to identify an Individual. Once data has been properly de-identified in accordance with HIPAA, it is no longer PHI and is not subject to this BAA.

2.14 **Mitigation.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of this BAA.

3. OBLIGATIONS OF COVERED ENTITY

3.1 **Permissions.** Covered Entity shall notify Business Associate of any limitations in the notice of privacy practices of Covered Entity under 45 C.F.R. § 164.520, to the extent that such limitations may affect Business Associate's Use or Disclosure of PHI.

3.2 **Restrictions.** Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an Individual to Use or Disclose his or her PHI, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI.

3.3 **Impermissible Requests.** Covered Entity shall not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity, except as expressly permitted for Business Associate under the HIPAA Rules or this BAA (for example, for data aggregation or management and administrative activities of Business Associate).

3.4 **Compliance.** Covered Entity represents and warrants that it has obtained and will obtain all necessary consents, authorizations, and permissions required under applicable law before providing PHI to Business Associate. Covered Entity is solely responsible for its own compliance with HIPAA and for ensuring that any instructions it provides to Business Associate regarding PHI are consistent with the HIPAA Rules.

3.5 **Safeguarding PHI on the SFDC Platform.** Covered Entity acknowledges that the Service Platform operates within Customer's Salesforce environment. Covered Entity is responsible for: (a) configuring user access controls and permissions within its Salesforce environment; (b) ensuring that its own Authorized Users do not create unencrypted custom fields or objects for high-risk PHI (such as Social Security numbers) outside of the Service Platform's managed package; (c) controlling what PHI is uploaded to or stored within the Service Platform; and (d) ensuring that third-party consultants, administrators, or applications granted access to Covered Entity's Salesforce environment comply with HIPAA. Business Associate shall have no liability for any Breach or unauthorized Disclosure of PHI caused by Covered Entity's or its agents' configuration of, or actions within, the SFDC Platform outside of the Service Platform's managed package.

3.6 **Third-Party Integrations.** To the extent Covered Entity enables integrations between the Service Platform and Third-Party Service Providers (as defined in the Agreement), Covered Entity is responsible for: (a) evaluating each Third-Party Service Provider's HIPAA compliance; (b) entering into a separate BAA with each such Third-Party Service Provider, as applicable; and (c) ensuring that PHI disclosed through such integrations is appropriately safeguarded. Business Associate's obligations under this BAA do not extend to PHI once it has been transmitted to a Third-Party Service Provider's systems.

4. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

4.1 **Service Performance.** Except as otherwise limited in this BAA, Business Associate may Use or Disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Agreement, provided that such Use or Disclosure would not violate the HIPAA Rules if done by Covered Entity.

4.2 **Business Associate's Own Management.** Business Associate may Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that any Disclosure of PHI for such purposes is Required by Law or Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that the information will remain confidential, be used or further disclosed only as Required by

Law or for the purposes for which it was disclosed, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4.3 **Aggregate and De-identified Data.** Business Associate may de-identify PHI in accordance with 45 C.F.R. § 164.514 and may use de-identified data for lawful purposes, including improvement of the Service Platform. De-identified data is not PHI and is not subject to the restrictions of this BAA.

5. TERM AND TERMINATION

5.1 **Term.** This BAA shall become effective on the Agreement Start Date and shall remain in effect for the duration of the Agreement Term. This BAA shall terminate automatically upon the termination or expiration of the Agreement, subject to Section 5.4.

5.2 **Termination for Cause.** Either Party may terminate this BAA if the other Party materially breaches a provision of this BAA and fails to cure such breach within thirty (30) business days after receiving written notice specifying the breach. If cure is not reasonably possible, the non-breaching Party may terminate this BAA immediately upon written notice.

5.3 **Effect of Termination of Agreement.** If the Agreement terminates for any reason, this BAA shall also terminate. Upon termination of this BAA for any reason, the provisions of Section 5.4 shall apply.

5.4 **Return or Destruction of PHI.** Upon termination of this BAA, Business Associate shall, at Covered Entity's election, return or destroy all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, in accordance with the data export and deletion provisions of the Agreement (including the Data Export Period and Data Deletion Period defined therein). To the extent that return or destruction is not feasible (for example, PHI stored in archived backups or retained to comply with legal obligations), Business Associate shall extend the protections of this BAA to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate retains such PHI. The obligations of this Section 5.4 shall survive the termination of this BAA.

6. LIABILITY AND INDEMNIFICATION

6.1 **Agreement Controls.** The limitation of liability, indemnification, and disclaimer provisions set forth in the Agreement (including the applicable liability cap) shall apply to this BAA and any claims arising hereunder, except to the extent that such limitations or exclusions are prohibited by the HIPAA Rules or other applicable law.

6.2 **Customer Responsibility.** Covered Entity acknowledges and agrees that Business Associate shall have no liability under this BAA for: (a) any failure by Covered Entity or its Authorized Users to comply with HIPAA; (b) any unauthorized Use or Disclosure of PHI by Covered Entity or its agents; (c) any Breach or Security Incident caused by the acts or omissions of Covered Entity's third-party consultants, contractors, or other agents operating within Covered Entity's Salesforce environment; or (d) PHI that Covered Entity transmits to or receives from a Third-Party Service Provider via integrations enabled by Covered Entity.

6.3 **SFDC Platform.** Business Associate shall not be liable for any Breach, Security Incident, unauthorized access, or loss of PHI to the extent caused by: (a) a failure of the SFDC Platform or Salesforce's infrastructure; (b) a security vulnerability in the SFDC Platform not attributable to Business Associate's application or managed package; or (c) any action or inaction by Salesforce with respect to the SFDC Platform. Covered Entity acknowledges that its Salesforce subscription agreement governs its relationship with Salesforce with respect to the SFDC Platform.

6.4 **Insurance.** Business Associate shall maintain commercially reasonable insurance coverage, which may include cyber liability or technology errors and omissions coverage, in amounts appropriate for a business of its size and scope of operations.

7. GENERAL PROVISIONS

7.1 **Amendment.** The Parties agree to take such action as is necessary to amend this BAA from time to time to comply with the requirements of the HIPAA Rules and any other applicable law. No amendment to this BAA shall be effective unless it is in writing and signed by both Parties.

7.2 **Interpretation.** Any ambiguity in this BAA shall be interpreted to permit compliance with the HIPAA Rules. In the event of a conflict between this BAA and the Agreement with respect to the protection of PHI, this BAA shall control.

7.3 **No Third-Party Beneficiaries.** Nothing in this BAA shall confer upon any person other than the Parties and their respective successors and permitted assigns any rights, remedies, obligations, or liabilities. Individuals whose PHI is subject to this BAA are not intended third-party beneficiaries.

7.4 **Governing Law and Dispute Resolution.** This BAA shall be governed by and construed in accordance with the governing law and dispute resolution provisions set forth in the Agreement. To the extent federal law (including HIPAA) conflicts with state law, federal law shall control.

7.5 **Notices.** All notices under this BAA shall be given in accordance with the notice provisions of the Agreement.

7.6 **Entire BAA.** This BAA, together with the Agreement, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior or contemporaneous oral or written agreements, understandings, or representations relating to the protection of PHI under HIPAA.

7.7 **Survival.** The obligations of Business Associate under Sections 2.3, 2.5, 2.6, 2.9, 2.10, and 5.4 of this BAA shall survive termination of this BAA for so long as Business Associate retains any PHI.

7.8 **Counterparts and Electronic Signatures.** This BAA may be executed in counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument. Electronic signatures shall be deemed valid and binding for all purposes.

IN WITNESS WHEREOF, the Parties have executed this Business Associate Agreement as of the date last signed below.

PROVIDER:	**CUSTOMER:**
BENELINX, LLC	[CUSTOMER LEGAL NAME]
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date Signed: _____	Date Signed: _____