**MASTER SERVICES AGREEMENT**

The following **MASTER SERVICES AGREEMENT**, including Exhibits attached hereto and made a part hereof (the “Agreement”) is made to be effective the \_21\_\_ day of \_\_\_\_January\_\_\_\_\_\_\_\_\_\_\_\_\_, 2025\_ (the “Effective Date”), by and between **\_\_\_ThriveAI LLC \_\_\_\_\_\_\_\_\_**, a corporation (“Service Provider”) and **HEALTHeLINK, Inc.**, a New York not-for-profit corporation (“HEALTHeLINK”) (Service Provider and HEALTHeLINK are sometimes referred to as “Parties”).

The Agreement between Service Provider and HEALTHeLINK consists of this Master Services Agreement and the following exhibits (and includes the schedules therein) which are incorporated by reference:

* Exhibit A: Statement(s) of Work/Fees
* Exhibit B: Change Order Form
* Exhibit C: Support and Maintenance Terms
* Exhibit D: Service Level Terms
* Exhibit E: Subcontractor Business Associate Agreement (“BAA”)
* Exhibit F: Data Security Addendum
* Exhibit G: Insurance Schedule

**RECITALS**

**WHEREAS**, HEALTHeLINK is a qualified entity (“QE”), operating primarily in the State of New York, which among other functions, facilitates the exchange of data among its stakeholders and participants (“Participants”). The Parties acknowledge that as a QE, HEALTHeLINK is a part of the Statewide Health Information Network for New York (“SHIN-NY”) administered by New York eHealth Collaborative, Inc., a New York not-for-profit corporation that serves as the designated entity of the New York State Department of Health (“DOH”) for the SHIN-NY; and

**WHEREAS**, HEALTHeLINK wishes to use one or more of Service Provider’s software, products, hardware or services. Service Provider is engaged in the business of developing, licensing and/or distributing software products and/or providing data related services to health care organizations and QEs. Service Provider offers these products and services under the terms of the Agreement.

**NOW THEREFORE**, in consideration of the foregoing, the covenants contained herein, and other good and valuable consideration, the receipt of which is hereby acknowledged, the Parties agree as follows:

1. **DEFINITIONS**.Unless otherwise defined in this Agreement, capitalized terms shall have the meaning given in the Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 NYCRR Section 300.3(b)(1), as amended from time to time (the “SHIN-NY Guidance”).
2. **SCOPE OF SERVICES.** 
   1. Services and Deliverables. Service Provider agrees to perform, directly or through its permitted Subcontractors, the services (“Services”) and/or deliver the deliverables (“Deliverables”) described in each Statement(s) of Work (“Statement of Work” or “SOW”), attached as **Exhibit A**. Each Statement of Work must be executed by duly authorized representatives of both Parties. Any revision to a SOW not otherwise requiring a new Statement of Work, shall be documented using the Change Order Form attached as **Exhibit B**.
   2. Support/Service Levels. If and as applicable, Services may include support and maintenance as set forth in **Exhibit C** (Support and Maintenance Terms). The Services may also be subject to service level agreements, which, if applicable, will be set out in **Exhibit D** (Service Level Terms).
   3. Use of Subcontractors. The Parties agree that Service Provider may use Subcontractors to provide Services under a Statement of Work only if pre-approved in writing by HEALTHeLINK. If HEALTHeLINK consents to use of a subcontractor, Service Provider shall ensure that such Subcontractor agrees in writing to the terms of this Agreement. Service Provider shall remain responsible for work performed by a permitted Subcontractor.
3. **PAYMENT TERMS.**
   1. Fees. In consideration for performing the Services and delivering the Deliverables, HEALTHeLINK shall pay Service Provider the fees, if any, (“Fees”) specified in the applicable Statement of Work(s), attached at **Exhibit A**, in accordance with the terms specified in the applicable Statement of Work.
   2. Invoices. Except as otherwise provided in a Statement of Work, within 15 days following the end of each month (or, with respect to the final invoice, within 30 days following the termination or expiration of this Agreement), Service Provider shall submit to HEALTHeLINK an invoice showing Services performed, Deliverables provided, and if applicable, approved expenses incurred during the preceding month, together with such supporting documentation as may be reasonably required by HEALTHeLINK. The invoice should be sent to HEALTHeLINK at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Service Provider shall perform the Services and delivery of the Deliverables in material compliance with the requirements of this Agreement as specified in the Statement of Work. HEALTHeLINK shall pay Service Provider all invoiced amounts that are not the subject of a good faith dispute within 30 days after receipt of an invoice.
   3. Cost Reimbursement. HEALTHeLINK shall pay Service Provider any out-of-pocket expenses preapproved by HEALTHeLINK in writing, which are reasonable and necessary for Service Provider to incur in furtherance of its performance hereunder, as set forth in a Statement of Work. Any approved cost reimbursement will be set out in the invoices provided by Service Provider and will be supported by documentation reasonably acceptable to HEALTHeLINK.
   4. Tax Exempt Status. HEALTHeLINK is a tax-exempt entity under federal and New York State law and will maintain such exemptions so long as this Agreement remains in effect. Upon request, HEALTHeLINK will provide Service Provider with evidence of its tax-exempt status.
4. **TERM AND TERMINATION.**
   1. Term.
      1. Agreement Term. The term of this Agreement will commence on the Effective Date and, unless modified by mutual agreement of the Parties or terminated earlier pursuant to the terms of this Agreement, shall continue until completion of all SOWs (the “**Term**”) or by mutual agreement of the Parties.
      2. Statement of Work Term. The term of each Statement of Work will commence on the effective date specified in that Statement of Work and, unless the Agreement is earlier terminated in accordance with this Section 4, shall continue in effect through the term specified in that Statement of Work.
   2. Termination For Cause. Either Party may terminate this Agreement or a Statement of Work, as applicable, if the other Party breaches any material term or commitment contained in this Agreement or the applicable Statement of Work, and the breach is not cured within 30 days upon receiving written notice from the breaching Party.
   3. Termination In Connection With Transfer, Dissolution, or Bankruptcy. Either Party may terminate this Agreement upon not less than 30 days’ notice in the event of either: (A) the winding up, transfer of substantially all of a Party’s assets, merger, or dissolution of a Party’s business or operations; or (B) the filing by a Party for protection under applicable bankruptcy or other debtor protection laws or regulations.
   4. Termination On 90 Days’ Notice. Either Party may terminate this Agreement without cause upon not less than 90 days’ notice to the other Party.
   5. Termination In Accordance With Subcontractor Business Associate Agreement. If applicable, either Party may terminate this Agreement in accordance with the BAA attached hereto as **Exhibit E**.
   6. Effect of Expiration or Termination. Upon the expiration or termination of this Agreement for any reason, HEALTHeLINK shall pay Service Provider only for Services and Deliverables provided and accepted by HEALTHeLINK prior to the date of expiration or termination. Except as expressly set forth herein or in a SOW, neither Party will have any other obligation or liability to the other Party in connection with any termination.
5. **RECORD RETENTION; AUDITS; REPORTS.**
   1. Record Retention. Service Provider shall retain records related to the subject matter of this Agreement (A) through the end of the 6th full calendar year after the end of the last fiscal year during which any Services or Deliverables are being provided by Service Provider to HEALTHeLINK through a Statement of Work or (B) if longer, such period as is required by applicable Laws (“Retained Records”). To the extent not in violation of Law or privacy rights of third parties, Service Provider shall at all times during the Term, and thereafter, make available, or cause to be made available, to HEALTHeLINK for inspection by its authorized representatives during regular business hours, at the place where such Retained Records are located, such Retained Records as are reasonably determined by HEALTHeLINK to be necessary (A) to perform and carry out its responsibilities hereunder, (B) for the defense of any legal or administrative action or claim arising under this Agreement and relating to any Retained Records or (C) to defend or prosecute any legal or administrative action or claim brought by or against a third party relating to the Statement of Work. HEALTHeLINK shall give Service Provider 10 days’ prior written notice of its need for any such records, and any such inspection shall be conducted without material interference with the operations of Service Provider.
   2. Regulatory Audits. In the case of an audit performed by or on behalf of any Regulatory Authority (a “Regulatory Audit”), which may be performed during business hours upon reasonable notice (in light of the prior notice, if any, provided by the applicable Regulatory Authority) each Party will provide to the Regulatory Authority or to the other Party for delivery to the Regulatory Authority the Retained Records and reasonable access to such Party’s facilities to the extent required by such Regulatory Authority.
6. **REPRESENTATIONS, WARRANTIES AND COVENANTS OF THE PARTIES.**
   1. Representations, Warranties and Covenants. Each Party hereby represents and warrants to the other Party that: (i) it has all requisite corporate power and authority to execute and deliver this Agreement, to consummate the transactions contemplated hereby and thereby, to grant any rights it purports to grant hereunder, and to perform its obligations hereunder in accordance with the terms hereof, and (ii) all necessary action required to have been taken by it or on its behalf has been taken to authorize the execution and delivery of this Agreement and the other agreements contemplated hereby, the consummation of the transactions contemplated hereby and thereby, the granting of any rights it purports to grant hereunder and thereunder, and the performance of its obligations hereunder and thereunder.
   2. Service Provider Representations and Warranties. Service Provider represents and warrants to HEALTHeLINK that Service Provider owns or properly licenses all technology and intellectual property rights in order to permit Service Provider to enter into and perform its obligations under this Agreement.
7. **CONFIDENTIALITY.**
   1. Each Party agrees and acknowledges that all books, manuals, documents, materials, processes, methods or other business or technical information in any form whatsoever, identified as confidential by a party (“Disclosing Party”) or which one would expect is proprietary, or which were distributed or otherwise disclosed to the other Party (“Receiving Party”), shall constitute “Confidential Information” under this Agreement.
   2. The Parties further acknowledge that each may have access to other Confidential Information of the other Party. Unless otherwise provided in a separate agreement between two or more of the Parties, each Party agrees to treat all information provided by the other Parties as confidential and privileged information, including the terms of this Agreement; not to share this information with anyone who is not associated with this Agreement; and not to use the information for any purpose other than for reasons related to the conduct of the work outlined in the Services.
   3. If, during the course of providing services under this Agreement, Service Provider accesses Protected Health Information, Personally Identifiable Information, or other confidential information relating to the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”) or applicable state law, such information shall be subject to the terms and conditions contained in the standard form of BAA attached as **Exhibit E**. Service Provider shall also comply with the provisions of the Data Security Addendum set out in **Exhibit F**.
8. **INTELLECTUAL PROPERTY AND DATA RIGHTS.**
   1. Service Provider owns and shall retain any and all rights, title and interest in the technology it provides under this Agreement and, except as provided herein, HEALTHeLINK shall not exercise any incidents of ownership or control or claim to own or control the Service Provider technology.
   2. HEALTHeLINK owns and shall retain any and all rights, title and interest in the technology and data it provides under this Agreement and, except as provided herein, Service Provider shall not exercise any incidents of ownership or control or claim to own or control the HEALTHeLINK technology or data.
   3. Except to the extent specifically set forth in a Statement of Work, all right, title and interest to the Deliverables shall belong to HEALTHeLINK as a “work for hire”.
   4. Unless pre-approved in writing by a Party, or as required by Law, neither Party may use the name, tradename, trademarks or service marks of the other Party.
9. **COMPLIANCE** **MATTERS**.
   1. Compliance with Laws. In the performance of its respective obligations under this Agreement, the Parties shall, to the extent and in the manner required by applicable Law, comply with all Laws to the extent applicable to the performance of such Person under this Agreement, including but not limited to HIPAA, the HITECH Act, 42 CFR Part 2, and the regulations, guidance, policies and procedures governing the SHIN-NY.
   2. Compliance with HIPAA. THE PARTIES ACKNOWLEDGE THAT TO THE EXTENT THE DATA CONSTITUTES PROTECTED HEALTH INFORMATION FOR PURPOSES OF HIPAA, IT MAY BE SUBJECT TO ADDITIONAL PROTECTIONS UNDER NEW YORK STATE LAW AND POLICIES. THE PARTIES WILL COMPLY WITH APPLICABLE LAWS WITH RESPECT TO ITS PROCESSING, USE OR DISCLOSURE OF ANY CLINICAL DATA CONSTITUTING PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE FORM OF THE BAA ATTACHED HERETO AS **EXHIBIT E**.
   3. Security. In cooperating with each other, the Parties shall implement security measures in accordance with applicable law and according to this Agreement, including, if applicable, the Data Security Addendum attached as **Exhibit F**. Should Service Provider or any of its professional staff become subject to an audit, investigation or review by the New York State Department of Health, the United States Department of Health and Human Services Office of the Inspector General, the New York State Deputy Attorney General for Medicaid Fraud, the New York State Medicaid Inspector General or any other regulatory, investigatory, or prosecutorial agency, Service Provider shall notify HEALTHeLINK immediately.
   4. Exclusion/Debarment. Service Provider represents that as of the Effective Date, and for the duration of the Term: (a) it is not listed by any federal or state agency as excluded, debarred, or otherwise ineligible for participation in any federal or state health care program, and that (b) it will not employ or directly contract with any individual or entity whom Service Provider knows or should have known after reasonable inquiry: (i) has been convicted of a criminal offense related to health care, or (ii) is then currently excluded, debarred or otherwise ineligible for participation in any federal or state health care program (unless the individual has been reinstated to participation in Medicare and all other federal and state health care programs after being excluded because of conviction). In furtherance of this requirement, Service Provider agrees that it shall make reasonable inquiry as to any existing or prospective employee, agent, subcontractor, or independent contractor considered for engagement by Service Provider to perform its obligations under this Agreement by reviewing the General Services Administration’s List of Parties Excluded from Federal Programs and the HHS/OIG Cumulative Sanction Report at least once (1x) per calendar year with respect to all such prospective and current employees, agents, subcontractors, and independent contractors, and shall notify HEALTHeLINK immediately in accordance with the notice provisions of this Agreement if it becomes aware of any such conviction, exclusion, debarment, or ineligibility. HEALTHeLINK shall have the right to terminate this Agreement immediately and, notwithstanding anything contained in this Agreement to the contrary, without penalty of any kind, upon becoming aware that Service Provider or its employee, agent, subcontractor, or independent contractor has been excluded or debarred, or at any time thereafter during which such entity or person continues to be excluded or disbarred, in HEALTHeLINK’s sole discretion.
10. **INDEMNIFICATION AND INSURANCE.**
    1. Insurance. Service Provider, at its sole cost and expense, shall at all times maintain liability and other insurances of such types and amounts set forth in **Exhibit G**.
    2. Indemnification and Liability. Service Provider (“Indemnifying Party”) shall: (i) indemnify and hold harmless HEALTHeLINK and its directors, officers and employees (the “Indemnified Party”) from and against any losses, damages or liabilities (including reasonable costs and expenses, and excluding attorneys’ fees, in each case, incurred by the Indemnified Party in connection with any third party claim, action, lawsuit, proceeding or investigations) (“Losses”) awarded or otherwise paid by the Indemnified Party to any third party (whether pursuant to a court order, or as part of a settlement approved by the Indemnifying Party) arising out of any action, suit, proceeding or other claim, or any threat thereof (whether civil, criminal, administrative, arbitral, investigative or otherwise) against any Indemnified Party (including by any Regulatory Authority); and (ii) shall be liable to the Indemnified Party for any direct damages (including any fines or penalties assessed by a governmental oversight entity and for which Indemnified Party is responsible), including reasonable costs and expenses, and attorneys’ fees, in each case, incurred by the Indemnified Party in connection with any third party claim, action, lawsuit, proceeding or investigations), not to include any indirect, consequential, special, incidental, or other exemplary losses or damages (“Damages”) suffered by the Indemnified Party, in each case to the extent:

(a) arising out of any failure of the Indemnifying Party to comply with Law in connection with its performance under this Agreement;

(b) relating to a violation of HIPAA or HITECH or any state law relating to data privacy by Indemnifying Party; or

(c) relating to a breach of this Agreement or the gross negligence or intentional misconduct of Indemnifying Party in connection with this Agreement.

* 1. Indemnification Procedure. If any claim is commenced against an Indemnified Party entitled to indemnification under Section 10.2, prompt notice thereof shall be given by the HEALTHeLINK to Service Provider. The Parties shall agree upon the Party who will be responsible for the defense of such claim; provided, however, that if the Parties cannot agree upon the Party who will be responsible for the defense of such claim within 15 days after receipt by the Indemnifying Party, (1) the Indemnifying Party shall immediately take control of the defense of such claim and shall engage attorneys acceptable to the HEALTHeLINK (which acceptance shall not be unreasonably withheld) to defend such claim; and (2) HEALTHeLINK shall cooperate with the Indemnifying Party (and its attorneys) in the defense of such claim. HEALTHeLINK may, at its own cost and expense, participate (through its attorneys or otherwise) in such defense. If the Indemnifying Party does not assume control over the defense of a claim as provided in this Section, HEALTHeLINK may defend the claim in such manner as it may deem appropriate, at the cost and expense of the Indemnifying Party. If the Indemnifying Party assumes control over the defense of a claim as provided in this Section, the Indemnifying Party may not settle such claim without the consent of the HEALTHeLINK, which consent will not be unreasonably withheld.

1. **DISPUTE RESOLUTION.**
   1. Informal Dispute Resolution.
      1. The Parties shall attempt to resolve all disputes arising out of or in any way connected with the execution, interpretation or performance of this Agreement, the performance or receipt of the Services or Deliverables hereunder or the relationship created hereby, in accordance with this Section 11.1.
      2. When a dispute arises between the parties relating to or in any way connected with the execution, interpretation or performance of this Agreement, the performance or receipt of the Services or Deliverables hereunder or the relationship created hereby: (i) Service Provider or HEALTHeLINK, as applicable, will send a notice to the other Party containing a detailed description of the issue under dispute, the good faith basis for the dispute and a recommendation for resolution; and (ii) within 15 days after receipt of such notice, the Parties will meet and confer in good faith at a mutually agreeable location to attempt to resolve the dispute promptly.
2. **MISCELLANEOUS.**
   1. No Assignment; Successors and Assigns. This Agreement may not be assigned by Service Provider without the prior written consent of HEALTHeLINK. This Agreement is binding upon, inures to the benefit of, and is enforceable by the Parties and their respective successors and assigns. The terms and provisions of this Agreement are intended solely for the benefit of each Party and its respective successors or permitted assigns, and it is not the intention of the Parties to confer third-party beneficiary rights upon any other person.
   2. Entire Agreement; Interpretation. This Agreement constitutes the entire agreement and understanding between the Parties with respect to the subject matter hereof and supersedes all prior agreements and understandings relating to the subject matter.
   3. Governing Law and Jurisdiction. This Agreement shall be governed by, and construed in accordance with, the internal laws of the State of New York applicable to contracts executed and performed in that state, without giving effect to choice-of-laws principles. With respect to any legal action, suit or proceeding by a Party arising out of this Agreement, each Party consents to the exclusive jurisdiction and venue of a United States District Court located in Erie County, New York, or other State Court of the State of New York located in or having jurisdiction over Erie County, New York.
   4. Independent Contractors. Notwithstanding any provision contained herein to the contrary, each of HEALTHeLINK and Service Provider understand and agree that the Parties hereto intend to act and perform as independent contractors and that therefore neither HEALTHeLINK nor Service Provider is an employee, partner, joint venturer, of the other. Nothing in this Agreement shall be construed as placing the Parties in a relationship of employer-employee, partners or joint venturers. Neither Party shall have the right to make any promises, warranties or representations, or to assume or create any obligations, on behalf of the other Party, except as otherwise expressly provided herein. HEALTHeLINK and Service Provider agree to be solely and entirely responsible for their respective acts and, to the extent provided under the Laws, for the acts of any of their respective officers, directors, employees, professional advisors (including accountants), contractors and other agents, except as otherwise expressly provided herein.
   5. Force Majeure. Service Provider and HEALTHeLINK shall not be liable to each other for any failure or delay in performance of this Agreement to the extent such failure or delay arises out of a cause beyond the reasonable control of such Party. Such causes may include, but shall not be limited to, acts of God, acts of a public enemy, acts of a civil or military authority, fires or other catastrophes, labor disputes, strikes, pandemics, delays in transportation or third-party delivery services, outages of a non-proprietary electrical or telecommunications network, riots or war, terrorism, changes in Regulatory Authority regulations (a “Force Majeure Event”).
   6. Notices. Any notice, demand or communication required, permitted, or desired to be given hereunder, unless otherwise stated, shall be deemed effectively given when personally received by the intended recipient, and shall be sent by (a) email or facsimile transmission with non-automatic acknowledgment (which need not satisfy the requirements of this Section) from the recipient indicating receipt; (b) express or overnight courier with proof of delivery; or (c) United States Postal Service, certified or registered mail with signed return receipt, addressed to the person or persons identified herein. Notwithstanding the foregoing, any notice of breach or termination must be sent by the method specified in clause (b) or (c) of this Section 13.6. Either Party may change the person and address to which notices or other communications are to be sent to it by giving written notice of any such change in the manner provided herein. The initial notification information is:

|  |  |
| --- | --- |
| **HEALTHeLINK Addresses for Notice:** | **Service Provider Addresses for Notice:** |
| 2475 George Urban Boulevard  Suite 202  Depew, New York 14043  Attn:  E-mail:  cc: Barclay Damon LLP  2000 Five Star Bank Plaza  100 Chestnut Street  Rochester, New York 14604  Attn: Bridget C. Steele, Esq.  bsteele@barclaydamon.com | ThriveAI  6381 Walnut Creek Dr,  East Amherst, NY  14051 |
|  |  |

* 1. Execution in Counterparts. This Agreement may be executed via DocuSign or other mutually acceptable electronic signature software, or in one or more counterparts, all of which, when taken together, shall constitute one and the same instrument. Delivery of an executed counterpart of a signature page to this Agreement by fax or electronic delivery in pdf format shall be as effective as delivery of a manually executed counterpart of this Agreement and shall be sufficient to bind the Parties to the terms and conditions hereof.
  2. Survival. The provisions of any other Section which by its nature or terms would be reasonably understood to have been intended to survive shall survive any termination or expiration of this Agreement.
  3. Severability. If any provision of this Agreement is determined by competent judicial authority to be invalid or unenforceable, that provision shall be deemed stricken herefrom and the remainder of this Agreement shall continue in full force and effect insofar as it remains a workable instrument to accomplish the intent and purposes of the Parties, as evidenced herein. In such an event, the Parties shall promptly replace the severed provision with the provision that will come closest to reflecting the intention of the Parties underlying the severed provision, but that is valid, legal, and enforceable.
  4. No Waiver. Waiver by a Party of any term or condition of this Agreement, or of any breach or default by the other Party hereunder, shall be effective only if made in writing and signed by an authorized representative of the Party waiving compliance herewith. Any such waiver so signed shall be effective only in the specific instance, and for the specific purpose, stated in such writing, and no waiver shall be deemed a waiver of any other term, condition, breach, or default, irrespective of whether similar to that waived. No failure to exercise, and no delay in exercising, on the part of either Party, any right, power, or privilege hereunder shall constitute a waiver thereof, nor will either Party’s exercise of any right, power, or privilege hereunder preclude further exercise of the same right, power, or privilege, or the exercise of any other right, power, or privilege, hereunder.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

**IN WITNESS WHEREOF**, the Parties hereto have caused this Agreement to be executed by their respective authorized signatories on the date first above written.

|  |  |
| --- | --- |
| ThriveAI | HEALTHeLINK, Inc. |
| Signature: Joseph A Eberle  Name: Joseph A. Eberle  Title: CEO | Signature:  Name:  Title: |

**EXHIBIT A**

**FORM FOR STATEMENT OF WORK**

Effective date: \_\_1/1/2025\_\_\_

**Description of Services/Products:**

**Development of AI exploration architecture and demonstration application.**

**Timeframe/Deliverables:**

**Demonstration 1 (month 2): AI exploration demonstration**

**Architecture Document and component storyboard**

**Demonstration 2 (month 4): AI exploration demonstration**

**Architecture Document and component storyboard**

**Demonstration 3 (month 6): AI exploration demonstration**

**Architecture Document and component storyboard**

**Demonstration 4 (month 8): Final AI exploration demonstration to State**

**Final Architecture Document and component storyboard to State**

**Fees/Timing and Method of Payment:**

**Time and materials billed monthly**

|  |  |
| --- | --- |
| ThriveAI LLC | HEALTHeLINK, Inc. |
| Signature: Joseph A. Eberle  Name: Joseph A. Eberle  Title: CEO | Signature:  Name:  Title: |

**EXHIBIT E**

**BUSINESS ASSOCIATE AGREEMENT (SUBCONTRACTOR)**

Effective as of the date of the latest signature below, (the “Effective Date”), and in connection with the Underlying Contact (as defined below), which requires \_ThriveAI\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, a \_\_LLC\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ located at \_\_\_6381 Walnut Creek Dr. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Service Provider”), to be provided with, to have access to, and/or to disclose Protected Health Information (as defined below) that is subject to regulations issued pursuant to the Health Insurance Portability and Accountability Act or 1996 (“HIPAA”) and its implementing regulations codified at 45 C.F.R. parts 160-164, as may be amended from time to time (the “Privacy and Security Rules”) and the Health Information Technology for Economic and Clinical Health Act and the regulations promulgated pursuant to such Act, including the Omnibus Rule effective September 23, 2013, as may be amended from time to time (“HITECH”) (HIPAA, the Privacy and Security Rules, HITECH and the Omnibus Rule together are the “HIPAA Rules”), this Subcontractor Business Associate Agreement (the “Agreement”) is made and entered into by and between Service Provider and HEALTHeLINK, Inc., a New York Not-for-Profit Corporation (“HEALTHeLINK”), in connection with Service Provider’s receipt, use, disclosure and creation of Protected Health Information with respect to the Underlying Contract. If an existing Business Associate Agreement exists between HEALTHeLINK and Service Provider (the “Existing BAA”), this Agreement is intended to replace any Existing BAA as of the Effective Date.

WHEREAS, HEALTHeLINK is a health information organization (“**HIO**”) that operates a health information exchange and record locator service to assist public and private health care providers, payers, and other health related organizations (the “**Participants**”) in locating and sharing patient information;

WHEREAS, the Participants, as covered entities under HIPAA have provided HEALTHeLINK with access to Protected Health Information, and HEALTHeLINK, as a Business Associate under HIPAA, has agreed to protect the privacy and security of such Protected Health Information, in accordance with HIPAA; and

WHEREAS, HEALTHeLINK wishes to engage Service Provider as a Subcontractor (defined below) to provide certain services (the “**Services**”), and in the course of such engagement, Service Provider may have access to and/or receive Protected Health Information originating from the Participants; and

WHEREAS, the parties hereto wish to restrict Service Provider’s use and disclosure of such Protected Health Information in accordance with this Agreement;

NOW, THEREFORE, HEALTHeLINK and Service Provider agree as follows:

1. **DEFINITIONS** Unless otherwise defined in this Agreement, any and all capitalized terms used in this Agreement have the meanings ascribed to them in the HIPAA Rules or the Underlying Contract.
   1. “Breach” has the same meaning as the term “Breach”, as defined in 45 C.F.R. § 164.402.
   2. “Business Associate” has the same meaning as the term “Business Associate”, as defined in 45 C.F.R. § 160.103.
   3. “Covered Entity” has the same meaning as the term “Covered Entity”, as defined in 45 C.F.R. § 160.103.
   4. “Data Aggregation Services” means the combining of PHI by Service Provider with the PHI received by Service Provider in its capacity as a Business Associate of a HIPAA covered entity, to permit data analyses that relate to health care operations of the respective covered entities.
   5. “Designated Record Set” has the same meaning as the term “Designated Record Set”, as defined in 45 C.F.R. § 164.501.
   6. “Electronic Protected Health Information” or “Electronic PHI” means information that comes within paragraphs 1(i) or 1(ii) of the definition of “Protected Health Information”, as defined in 45 C.F.R. § 160.103.
   7. “Individual” has the same meaning as the term “Individual”, as defined in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502.
   8. “Medicaid Confidential Data” or “MCD” means any information or data received directly or indirectly from the New York Department of Health (“**DOH**”) about individuals who have applied for or received Medicaid benefits, including Medicaid claims data, names and addresses, diagnoses, medical services, and other personally identifiable information. MCD may include Protected Health Information.
   9. “Protected Health Information” or “PHI” has the same meaning as the term “Protected Health Information”, as defined in 45 C.F.R. § 160.103. “Protected Health Information” includes without limitation “Electronic Protected Health Information” as defined above.
   10. “Security Incident” has the same meaning as the term “Security Incident”, as defined in 45 C.F.R.

§ 164.304.

* 1. “Statewide Health Information Network of New York” or “SHIN-NY” means the set of agreements (and the transactions, relations and data that are created by and through such set of agreements), between the New York State Department of Health, the New York eHealth Collaborative, Inc., HEALTHeLINK and other health information organizations and their participants, to make possible the exchange of clinical information among authorized users for authorized purposes to improve the quality, coordination and efficiency of patient care, reduce medical errors and carry out public health and oversight activities, while protecting privacy and security.
  2. “SHIN-NY Policy Guidance” means a set of policies and procedures, including technical standards and SHIN-NY services and products that are approved by the New York State Department of Health, related to the operation of the SHIN-NY.
  3. “Subcontractor” has the same meaning as the term “Subcontractor”, as defined in 45 C.F.R. § 160.103.
  4. “Underlying Contract” means any existing or future agreement entered into by and between Service Provider and HEALTHeLINK.
  5. “Unsecured Protected Health Information“ or “Unsecured PHI” has the same meaning as the term “unsecured protected health information” as defined in 45 C.F.R. § 164.402.

# OBLIGATIONS OF THE PARTIES WITH RESPECT TO PHI

* 1. Obligations of Service Provider. With regard to its use and/or disclosure of PHI, Service Provider agrees to:
     1. Not use or disclose the PHI other than as permitted or required by this Agreement or the Underlying Contract or as required by applicable law, rule or regulation, or by accrediting or credentialing organization to whom HEALTHeLINK is required to disclose such information or as otherwise permitted under the Statewide Policy Guidance, or the Privacy and Security Rules.
     2. Implement and use appropriate safeguards to prevent the use or disclosure of the PHI other than as provided for by this Agreement. Without limiting the generality of the foregoing sentence, Service Provider will:
        1. Implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI as required by the Privacy and Security Rules;
        2. Ensure that any agent, including a subcontractor, to whom Service Provider provides Electronic PHI agrees to implement reasonable and appropriate safeguards to protect Electronic PHI; and
        3. Promptly (but in no event later than 15 days after discovery (as defined in 45 C.F.R. § 164.410(a)(2)) thereof) report to HEALTHeLINK any Security Incident of which Service Provider becomes aware. Any notice of a Security Incident shall include the identification of each Individual whose Protected Health Information has been, or is reasonably believed by Service Provider to have been, accessed, acquired, or disclosed during such Security Incident as well as any other relevant information regarding the Security Incident, in each case to the extent such information is available to Service Provider and promptly after (but in no event later than 10 days after discovery (as defined in 45 C.F.R. § 164.410(a)(2)) thereof) such information becomes known to Service Provider.

Notwithstanding, the Parties agree that for purposes of this Subsection 2.1.b(iii), it shall not be necessary to report Unsuccessful Security Incidents (as defined below) unless requested by HEALTHeLINK. “Unsuccessful Security Incidents” shall include, but not be limited to, pings and other broadcast attacks on HeL’s firewall, port scans, unsuccessful log-in attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

* + 1. Promptly report to HEALTHeLINK, and mitigate, to the extent practicable, any harmful effect that is known to Service Provider of any use or disclosure of PHI by Service Provider in violation of the requirements of this Agreement and/or any Security Incident or Breach, and take steps to avoid any further similar violating uses or disclosures and/or Security Incidents or Breaches.
    2. Report to HEALTHeLINK any Breach of Unsecured PHI immediately after (but in no event later than 10 days after discovery (as defined in 45 C.F.R. § 164.410(a)(2)) of such Breach) the discovery (as defined in 45 C.F.R. § 164.410(a)(2)) of such Breach and provide to HEALTHeLINK notice of all of the elements specified in 45 C.F.R. § 164.404(c) (to the extent such information is available to Service Provider) promptly after (but in no event later than 10 days after discovery (as defined in 45 C.F.R. § 164.410(a)(2)) of such Breach) such information becomes known to Service Provider, including, to the extent possible, the identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Service Provider to have been, accessed, acquired or disclosed during such Breach. Service Provider shall cooperate and assist HEALTHeLINK, at no cost to HEALTHeLINK only to the extent such Breach is caused by or resulting from the acts or omissions of Service Provider, its subcontractors or agents, in making notification as required by law in the event of a Breach due to Service Provider.
    3. Service Provider shall cooperate and assist HEALTHeLINK in the reasonable investigation of any violation of the requirements of this Agreement and/or any Security Incident or Breach at no cost to HEALTHeLINK to the extent such violation, Security Incident and/or Breach is caused by or resulting from the acts or omissions of Service Provider, its subcontractors or agents.
    4. Ensure that all of its subcontractors and agents that receive, use, or have access to PHI agree, in writing, to the same restrictions and conditions on the use and/or disclosure of PHI that apply through this Agreement to Service Provider with respect to such information. HEALTHeLINK acknowledges that such writing may differ in form, but will not differ in substance from this Agreement. If Service Provider becomes aware of a pattern of activity or practice of a subcontractor or agent that would constitute a material breach or violation of the subcontractor's or agent’s obligations under such writing, Service Provider shall take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, terminate the contract or arrangement, if feasible.
    5. Upon 5 days’ written notice by HEALTHeLINK, provide access to PHI in a Designated Record Set to HEALTHeLINK or, as directed by HEALTHeLINK, to an Individual in order to meet applicable access requirements of the Privacy and Security Rules. If HEALTHeLINK is required to provide access to PHI in a Designated Record Set in a specific format, Service Provider will provide access to PHI in such format to the extent Service Provider maintains PHI in such format in accordance with Section 13405(e) of the HITECH Act. If an Individual makes a request for access to PHI directly to Service Provider, Service Provider shall notify HEALTHeLINK of the request within 3 business days of such request and will cooperate with HEALTHeLINK and allow HEALTHeLINK to send the response to the Individual.
    6. Upon 5 days’ written notice by HEALTHeLINK, make, or make available for, amendment(s) to PHI in a Designated Record Set that HEALTHeLINK directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of HEALTHeLINK or an Individual. If an Individual makes a request for an amendment to PHI directly to Service Provider, Service Provider shall notify HEALTHeLINK of the request within 3 business days of such request and will cooperate with HEALTHeLINK and allow HEALTHeLINK to send the response to the Individual.
    7. Subject to attorney-client and any other applicable legal privilege, make its internal practices, books and records, including policies and procedures relating to the use and disclosure of PHI, available to the Secretary of the U.S. Department of Health and Human Services (“**HHS**”) or his/her designee, in the reasonable time and manner specified by the Secretary, for purposes of the Secretary determining compliance of HEALTHeLINK with the HIPAA Rules. Subject to the legal privileges referred to above and as otherwise permitted by law, Service Provider shall, within 15 business days after receipt of such request, notify HEALTHeLINK of any request for access by HHS and shall provide HEALTHeLINK with a copy of the HHS request for access and all materials to be disclosed pursuant thereto.
    8. Document such disclosures of PHI as would be required for HEALTHeLINK to respond, in accordance with the HIPAA Rules, to a request by any Individual for an accounting of disclosures of PHI in accordance with the requirements of the HIPAA Rules.
    9. Upon 5 days’ written notice by HEALTHeLINK, make available or provide to HEALTHeLINK or the Individual information collected in accordance with Section 2.1(j), to permit HEALTHeLINK to respond, in accordance with the HIPAA Rules, to a request by an Individual for an accounting of disclosures of PHI. If an Individual makes a request for an accounting directly to Service Provider, Service Provider shall notify HEALTHeLINK of the request within 3 business days of such request and will cooperate with HEALTHeLINK and allow HEALTHeLINK to send the response to the Individual.
    10. Upon written notice by HEALTHeLINK that the Underlying Contract will be terminated for any reason, return to HEALTHeLINK or destroy and, unless return or destruction is infeasible, certify to HEALTHeLINK in writing of any such destruction, within thirty (30) days of Service Provider’s receipt of such notice, all PHI obtained from HEALTHeLINK or created or obtained by Service Provider on behalf of HEALTHeLINK with respect to the Underlying Contract, including such PHI that is in the possession of Service Provider’s subcontractors and agents, and retain no copies if it is feasible to do so; provided, however, that prior to destroying or returning PHI, the Parties will meet and confer in order to reach a mutually satisfactory resolution with respect to the feasibility of destroying or returning the PHI and Service Provider’s right to continued use and disclosure of the PHI. If return or destruction of the PHI is infeasible as reasonably determined by the Parties and/or Service Provider, Service Provider shall extend all protections contained in this Agreement to Service Provider’s use and/or disclosure of any retained PHI, and limit any further uses and/or disclosures to the purposes mutually agreed upon by the Parties. This Provision shall apply to PHI that is in the possession of subcontractors or agents of Service Provider.
    11. Comply with HITECH as applicable to Service Provider.
    12. To the extent Service Provider is required to carry out HEALTHeLINK’ obligations under 45 C.F.R. subpart E, comply with the requirements of such subpart that apply to HEALTHeLINK in the performance of such obligations, including, but not limited to, minimum necessary and document retention standards.
    13. In receiving, storing, processing, or otherwise dealing with any “patient identifying information” or “records” as defined in 42 C.F.R. § 2.11, from an alcohol/drug abuse “program,” as defined in 42 C.F.R. § 2.11, that is federally assisted in a manner described in 42 C.F.R. § 2.12(b), and that is operated by Covered Entity, to be fully bound by the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2.
    14. Resist in judicial proceedings any efforts to obtain access to “patient identifying information” or “records” as defined in 42 C.F.R. § 2.11 and as maintained by Service Provider, other than as permitted by the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2.
    15. Comply with all applicable federal and state laws and regulations governing the confidentiality of information provided by HEALTHeLINK including, without limitation, New York Public Health Law §§ 18 (Access to Patient Information) & 2780 et seq.; New York Mental Hygiene Law §§ 22.05 & 33.13; New York Civil Rights Law § 79-l; New York General Business Law §§ 399-dd (Confidentiality of Social Security Account Number), 399-h, & 899-aa; New York Civil Practice Law and Rules (CPLR) §§ 2302(a), 4504, 4507, 4508, & 4510 and CPLR R. 3122(a); chapter 5 of title 10 of the Official Compilation of Codes, Rules, and Regulations of the State of New York (NYCRR); 10 NYCRR § 63.6(k); Federal Rules of Evidence R. 501; and 21 C.F.R. § 1304.24(d).
    16. Pursuant to New York General Business Law § 899-aa(2)&(3) and in conformity with paragraph 2.1(a) of this Agreement, within 15 days’ after discovery thereof, notify HEALTHeLINK of any “breach of the security of the system,” as defined in New York General Business Law § 899-aa(1)(c), that involves PHI containing individuals’ “private information,” as defined in New York General Business Law § 899- aa(1)(b), that was, or was reasonably believed to be, acquired from Service Provider by a person without valid authorization.
    17. In the event Service Provider chooses to destroy the PHI in its possession in compliance with paragraph 2.1(l) of this Agreement, and that PHI contains “personal identifying information” as defined in New York General Business Law § 399-h(1)(d), dispose of such information in conformity with New York General Business Law § 399-h(2).
  1. Permitted Uses and Disclosures of PHI by Service Provider. Except as otherwise specified in this Agreement, Service Provider may use and disclose the PHI as reasonably necessary to perform its obligations under the Underlying Contract, including, use and disclosure described in the NDA, provided that such use or disclosure does not violate the HIPAA Rules. Unless otherwise limited herein, Service Provider may:
     1. Use the PHI in its possession for its proper management and administration of Service Provider, and to carry out the required legal responsibilities of Service Provider.
     2. Disclose the PHI in its possession to a third party for the purpose of Service Provider’s proper management and administration or to carry out the legal responsibilities of Service Provider, provided that the disclosures are required by law or Service Provider obtains written assurances from the person to whom the information is disclosed that 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 person, and the person notifies Service Provider of any instances of which it is aware in which the confidentiality of the information has been breached. Such written assurances shall include adherence to the same restrictions and conditions on use and disclosure as apply to Service Provider herein. HEALTHeLINK acknowledges that such written assurances may differ in form, but will not differ in substance, from this Agreement.
     3. Provide Data Aggregation Services as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B) and the Underlying Contract.
     4. Use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1). To the extent permitted by applicable law, prior to disclosing PHI as required by law to a law enforcement, regulatory, administrative, or oversight agency, or in response to a subpoena, court order, civil investigative demand, or other compulsory document or lawful process, Service Provider shall notify HEALTHeLINK of such pending disclosure and provide reasonable time for HEALTHeLINK to oppose such disclosure, should HEALTHeLINK deem such opposition necessary; provided, however, that if HEALTHeLINK does not respond to Service Provider regarding such opposition prior to the date on which such disclosure must be made, Service Provider may, in its own discretion, disclose PHI as required by law.
  2. Prohibited Uses and Disclosures of PHI by Service Provider. Service Provider shall neither use nor disclose Protected Health Information except as permitted or required by this Agreement. Specifically, without limitation, this Agreement does not authorize Service Provider to:
     1. Sell Protected Health Information for any purpose;
     2. Use or disclose Protected Health Information for Marketing purposes;
     3. Receive, maintain, store, access or transmit PHI outside of the United States and its territories; or
     4. Unless specifically permitted in the Underlying Agreement or otherwise agreed to by HEALTHeLINK in advance in writing, Service Provider shall not de-identify Protected Health Information.
  3. Obligations of HEALTHeLINK. By acceptance hereof, HEALTHeLINK agrees:
     1. To notify Service Provider of any restriction, or change in any restriction, to the use or disclosure of Protected Health Information that HEALTHeLINK has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Service Provider’s use or disclosure of PHI.
     2. To notify Service Provider of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Service Provider's use or disclosure of PHI.
     3. Not to request Service Provider to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by HEALTHeLINK.
  4. Obligations Relating to MCD. The Parties understand and acknowledge that this Section 2.5 only applies if Service Provider shall be given access to MCD in the course of providing services to HEALTHeLINK pursuant to the Underlying Contract.

The Federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between the Department of Health and any second party that will receive MCD must include contract language that will bind such parties to ensure that contractor(s)/business associates abide by the regulations and laws that govern the protection of individual, Medicaid confidential level data. This requires that you include the following language in this contract and all future contracts that will govern the receipt and release of such confidential data:

*Medicaid Confidential Data/Protected Health Information (MCD/PHI) includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information. You must comply with the following state and federal laws and regulations:*

* *Section 367-b(4) of the NY Social Services Law*
* *New York State Social Services Law Section 369 (4)*
* *Article 27-F of the New York Public Health Law and 18 NYCRR 360-8.1*
* *Social Security Act, 42 USC 1396a (a)(7)*
* *Federal regulations at 42 CFR 431.302, 42 CFR Part 2*
* *The Health Insurance Portability and Accountability Act (HIPAA), and HITECH at 45 CFR Parts 160 and 164*
* *Section 33.13 of the New York State Mental Hygiene Law*
* *SHIN-NY Regulation: 10 NYCRR Part 300.*

*Please note that MCD released to you may contain AIDS/HIV related confidential information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5)(a), the following notice is provided to you:*

*"This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure."*

*Alcohol and Substance Abuse Related Confidentiality Restrictions:*

*Alcohol and substance abuse information is confidential pursuant to 42 CFR Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.*

*You agree to ensure that you and any agent, including a subcontractor/business associate, to whom you provide MCD/PHI, agrees to the same restrictions and conditions that apply throughout this Agreement. Further, you agree to state in any such agreement, contract or document that the party to whom you are providing the MCD/PHI may be required to provide their Business Associate Agreements to DOH and may be required to receive acknowledgement or written agreement from DOH prior to redisclosing the MCD. You agree to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that you enter into that involves MCD/PHI.*

*Any agreement, contract, or document with a subcontractor/business associate must contain all of the above provisions pertaining to confidentiality. It must contain the HIV/AIDS notice as well as a statement that the subcontractor/business associate may not use or disclose the MCD without the prior written approval of DOH.*

*Any MCD provided under this Agreement shall not be accessed by employees, agents, representatives, or contractors/business associates who are located outside of the United States and its territories (offshore). Further, MCD shall not be received, stored, processed, or disposed via information technology systems which are located offshore.*

# TERMINATION

* 1. Termination Generally. This Agreement shall terminate when all of the PHI obtained from HEALTHeLINK or created or obtained by Service Provider on behalf of HEALTHeLINK, is destroyed or returned to HEALTHeLINK, or, if it is not feasible to return or destroy the PHI, protections are extended to such information in accordance with Section 2.1(l).
  2. HEALTHeLINK’s Right to Terminate for Cause. Upon HEALTHeLINK’s knowledge of a material breach by Service Provider of the terms of this Agreement, HEALTHeLINK shall either:
     1. Provide an opportunity for Service Provider to remediate the material breach of the terms of this Agreement or end the violation. If Service Provider does not remediate the material breach of the terms of this Agreement or end the violation within the time specified by HEALTHeLINK, HEALTHeLINK shall terminate: (A) this Agreement; (B) all of the provisions of the Underlying Contract that involve the use or disclosure of PHI; and (C) such other provisions, if any, of the Underlying Contract as HEALTHeLINK designates in its sole discretion;
     2. If Service Provider has breached a material term of this Agreement and remediation is not possible, immediately terminate: (A) this Agreement; (B) all of the provisions of the Underlying Contract that involve the use or disclosure of PHI; and (C) such other provisions, if any, of the Underlying Contract as HEALTHeLINK designates in its sole discretion.

# INDEMNITY

Service Provider shall indemnify and hold HEALTHeLINK, its directors, officers, affiliates and employees, harmless against all claims and costs resulting from acts/omissions of Service Provider in connection with its obligations under this Agreement. Service Provider shall be fully liable for the actions of its agents, employees, partners or subcontractors and shall fully indemnify and save harmless HEALTHeLINK from suits, actions, damages and costs, of every name and description relating to breach notification required by 45 CFR Part 164, Subpart D, caused by any intentional act or negligence of Service Provider, its agents, employees, partners or subcontractors, without limitation; provided, however, that Service Provider shall not indemnify for that portion of any claim, loss or damage arising hereunder due to the negligent act or failure to act by HEALTHeLINK.

# MISCELLANEOUS

* 1. Regulatory References. A reference in this Agreement to a section in HIPAA, the HIPAA Rules means the section as in effect or as amended or modified from time to time, including any corresponding provisions of subsequent superseding laws or regulations.
  2. Interpretation. The terms of this Agreement shall prevail in the case of any conflict with (a) Underlying Contract or (b) the Statewide Policy Guidance, in each case, to the extent necessary to allow HEALTHeLINK to comply with the HIPAA Rules and shall be construed in such a manner as to be permissible under the HIPAA Rules. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Rules, as amended, the HIPAA Rules shall control. Where provisions of this Agreement are different than those mandated in the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of this Agreement shall control.
  3. Survival. Notwithstanding any other provision of this Agreement to the contrary, the terms of this Agreement shall survive its termination and continue indefinitely solely with respect to any PHI Service Provider retains in accordance with this Agreement.
  4. No Third Party Beneficiaries. Except as expressly stated herein or the Privacy Rule, Service Provider and HEALTHeLINK do not intend to create any rights in any third parties. Nothing in this Agreement shall confer upon any person other than Service Provider and HEALTHeLINK and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
  5. Effect. This Agreement shall be binding upon, and shall inure to the benefit of, the parties hereto and their respective successors and assigns.
  6. Governing Law; Jurisdiction. This Agreement shall be governed by the laws of the State of New York and shall be enforceable in the courts of the State of New York, Erie County, or in the United States District Court for the Western District of New York. Service Provider, and by acceptance hereof, HEALTHeLINK, irrevocably submit to the exclusive jurisdiction of such courts.
  7. Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for HEALTHeLINK to comply with the requirements of the HIPAA Rules and other applicable law or regulation.
  8. Terms. The terms of this Agreement are hereby incorporated into the Underlying Contract and supplement and/or amend the Underlying Contract as required (and only as required) to allow HEALTHeLINK to comply with the HIPAA Rules and other applicable laws. The terms of the Underlying Contract that are not modified by this Agreement shall remain in full force and effect in accordance with the terms thereof. The Underlying Contract, this Agreement, the Statewide Policy Guidance as applicable to Service Provider, and any amendments thereto, constitute the entire agreement of the parties with respect to the subject matter contained herein.
  9. Ownership of PHI. Except as specified in Section 2.2 above or as otherwise agreed to in writing by both parties, as between HEALTHeLINK and Service Provider, HEALTHeLINK holds all right, title and interest in and to any and all PHI received by Service Provider from, or created or received by Service Provider on behalf of, HEALTHeLINK, and Service Provider does not hold, and will not acquire by virtue of this Agreement or by virtue of providing any services or goods to HEALTHeLINK, any right, title or interest in or to such PHI or any portion thereof.
  10. Illegality. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect.
  11. Notices. Any notice, demand or communication required, permitted, or desired to be given hereunder, unless otherwise stated, shall be deemed effectively given when personally received by the intended recipient, and shall be sent by (a) express or overnight courier with proof of delivery; or (b) United States Postal Service, certified or registered mail with signed return receipt, addressed to the person or persons identified herein. Either Party may change the person and address to which notices or other communications are to be sent to it by giving written notice of any such change in the manner provided herein. The initial notification information is:

|  |  |
| --- | --- |
| **HEALTHeLINK Addresses for Notice:** | **Service Provider Addresses for Notice:** |
| HEALTHeLINK, Inc.  2475 George Urban Blvd, Suite 202  Depew, NY 14043  Attn: Patricia A. Burandt  Privacy Officer  Email: [pburandt@wnyhealthelink.com](mailto:pburandt@wnyhealthelink.com) | Service Provider Name:  ThriveAI  Address: 6381 Walnut Creek Dr.  East Amherst, NY, 14051  Attn: Joseph A. Eberle  Title: CEO  Email: josepheberle@outlook.com |
| *with a copy to:*  Barclay Damon LLP  2000 Five Star Bank Plaza  100 Chestnut Street  Rochester, New York 14604  Attn: Bridget C. Steele, Esq. [bsteele@barclaydamon.com](mailto:%20bsteele@barclaydamon.com) | *with a copy to:* |

* 1. Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile and electronic copies thereof shall be deemed originals.
  2. Independent Contractors. Notwithstanding any provision contained herein to the contrary, each of Service Provider and HEALTHeLINK understand and agree that the parties hereto intend to act and perform as independent contractors and that therefore neither Service Provider nor HEALTHeLINK is an employee, partner, joint venturer, of the other. Nothing in this Agreement shall be construed as placing the parties in a relationship of employer-employee, partners or joint venturers. Neither Service Provider nor HEALTHeLINK shall have the right to make any promises, warranties or representations, or to assume or create any obligations, on behalf of the other party, except as otherwise expressly provided herein. Service Provider and HEALTHeLINK agree to be solely and entirely responsible for their respective acts and, to the extent provided under the laws, for the acts of any of their respective officers, directors, employees, professional advisors (including accountants), contractors and other agents, except as otherwise expressly provided herein.

[REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

IN WITNESS WHEREOF, the parties hereto have caused this Subcontractor Business Associate Agreement to be executed by their respective authorized signatories on the date first above written.

|  |  |
| --- | --- |
| **HEALTHeLINK, INC.** | **ThriveAI LLC** |
| By:  Print Name: Jennifer Lane  Title: Vice President, Technology  Address: 2475 George Urban Blvd Suite 202  Depew, NY 14225  Date: , | By: Joseph A. Eberle  Print Name: Joseph A. Eberle  Title: CEO  Address: 6381 Walnut Creek Dr.  East Amherst, NY 14051    Date:1/21/2025 |

**EXHIBIT F**

**DATA SECURITY ADDENDUM**

This Exhibit F (“**Exhibit**”) sets forth this Data Security Addendum, which is incorporated into the attached \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and Business Associate Agreement Exhibit (together, the “**Agreement**”) between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**Vendor**”) and HEALTHeLINK, Inc (“**Customer**”). The capitalized terms in this Exhibit shall have the meanings provided for such terms in the Agreement unless otherwise defined in this Exhibit. This Exhibit does not limit Vendor’s confidentiality, data privacy or other information security requirements under the Agreement, or any other agreement between the parties.

1. **OBLIGATIONS ARISING FROM THE ACQUISITION AND HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION**

Vendor shall process the Personally Identifiable Information and/or Sensitive Personally Identifiable Information provided by Customer and use any Customer data and assets only as permitted or required pursuant to the Agreement, and will only do so: (i) for the benefit of Customer as set forth in the Agreement, or as instructed by Customer from time to time in writing; (ii) as needed by Vendor to the extent strictly necessary to perform Vendor's obligations under the Agreement; and (iii) as otherwise required or permitted by applicable law and in accordance with the Business Associate Agreement between the parties.

For purposes of this Exhibit, “Personally Identifiable Information” or “PII” shall mean any information that, alone or in any combination with other information can be used to identify, locate, or contact an individual, including, without limitation, an individual’s name, address, social security number, educational or medical records, email address, credit card number and any other data that constitutes “personal information”; and “Sensitive Personally Identifiable Information” or “SPII” shall mean any Personally Identifiable Information that requires additional security under applicable data protection legislation as a result of its sensitive nature to the individual, including, without limitation, all Protected Health Information as defined under HIPAA, information concerning an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, physical or mental health, sexual orientation, criminal record, financial account numbers, medical records, biometric information, date of birth, and/or government-issued identification numbers (such as U.S. Social Security numbers or other national insurance or identification numbers, driver’s license numbers, and passport numbers).

In processing Customer's PII and/or SPII, Vendor will not: (i) disclose it to unaffiliated third parties unless expressly permitted to do so by Customer; (ii) transfer it across international borders; or (iii) do any other action that may in any manner adversely affect the integrity or confidentiality of such PII and/or SPII, other than as expressly specified herein or as directed by Customer in writing. Vendor agrees to ensure security requirements and obligations within this Exhibit and pursuant to the Agreement are extended to all subcontractors.

1. **MAINTAIN AN INFORMATION SECURITY PROGRAM**

Vendor agrees to establish, maintain, and follow a written information security program with appropriate information security safeguards that will remain active and in place through the term of the Agreement, which is designed to: (i) protect the confidentiality, integrity and availability of Customer’s systems and data exchanged pursuant to the Agreement from unauthorized access, use, or disclosure, or any other anticipated threats or hazards; and (ii) meet or exceed the requirements contained in regulations and common industry standards, such as HIPAA, HITECH, consistent with the security and privacy policies and standards set forth in 45 CFR 155.260(b) and any other relevant regulation or law (collectively the “**Information Security Program**”). Vendor shall provide Customer with a written plan for continuous monitoring of security control effectiveness. Vendor agrees that its Information Security Program will include the specific areas outlined below.

1. Mandatory Training and Screening. Vendor agrees that the Information Security Program will include mandatory and regular security and privacy training for all of Vendor’s staff, contractors, agents or representatives who have access to PII or SPII. Vendor shall provide screening results or allow Customer to conduct background checks for all of Vendor’s staff, contractors, agents or representatives who have access to PII or SPII.
2. Notification and Assistance in Handling PII and/or SPII. Vendor shall notify Customer within five business days and provide its full cooperation and assistance in relation to any complaint, inquiry or request made with respect to any PII or SPII related to the Agreement, by: (i) providing Customer with full details of the complaint, inquiry or request; (ii) complying with a data subject access request within the relevant timelines set out in any data protection legislation; and (iii) providing Customer with any PII or SPII it holds in relation to an individual making a complaint, inquiry or request, within the reasonable timelines required by Customer.
3. Implement Strong Access Control Measures. Vendor agrees to implement strong access control measures (the “Measures”) by implementing secure logon procedures including administrative, technical and physical controls to systems and data. Such Measures include a strong password management program and limiting access based on job responsibility, business need, and the performance of the obligations contained in any agreement executed between the parties. User access privileges to systems and applications must be reviewed at least quarterly for every year of the term. Access privileges shall be terminated within twenty-four (24) hours of any employee departing Vendor’s employment, or changing job responsibilities wherein access to the systems and applications are no longer required. Vendor shall notify Customer promptly, within 24 hours, after a change in employment, access rights and/or responsibilities affecting Vendor’s workforce and relative to any and all services provided by Vendor to Customer under the Agreement (the “Services”). Vendor shall cause all Customer data to be stored within the United States, and Vendor shall not store, transfer, or access any Customer data outside of the United States. Vendor’s information systems that receive, process, store, or transmit information are located [PROVIDE ADDRESSES FOR ALL PHYSICAL LOCATIONS].
4. Maintain a Vulnerability Management Program and Disaster Recovery Plan. Vendor agrees to keep all operating systems, firewalls, routers, servers, personal computers and all other systems current with appropriate system patches and updates in keeping with industry best practices and commercially reasonable security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs. Throughout the term of this Agreement, Vendor shall maintain a disaster recovery plan and conduct at least annual training to ensure competence and readiness to implement such plan, and be ready and able to immediately implement such plan. At Customer’s request, Vendor shall provide a copy of such disaster recovery plan to Customer.
5. Protect Data. Vendor agrees to develop, employ, and document processes, procedures, and/or templates designed to ensure that both parties' systems and Customer’s data exchanged pursuant to the Agreement are protected throughout the entire System Development Life Cycle (SDLC) (collection, transformation, use, storage and secure destruction) regardless of the media used to store the data, and will do so pursuant to the sensitivity classification of that data (e.g., Protected Health Information). Vendor agrees to implement the Measures necessary to protect all data exchanged pursuant to the Agreement, wherein such Measures include using strong encryption of all PII and/or SPII exchanged or generated pursuant to the Agreement when stored electronically on any of either parties' systems including but not limited to laptops, tablets, personal computers, servers and/or databases, at rest and/or in transit. Vendor’s encryption controls shall include cryptographic security in compliance with the Federal Information Processing Standard 140-2.
6. Maintain Secure Networks. The parties agree to maintain secure networks by protecting all Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best practices and commercially reasonable security practices. Vendor agrees that access to firewalls and servers must be accomplished through a secure connection only, and agree to maintain controls against malicious code and technical vulnerabilities through formal policies.
7. Regularly Monitor and Test Networks. Vendor agrees to regularly monitor and test its networks on its information systems (e.g., monitor and test using port scanning, virus scanning, internal/external vulnerability scanning), and to ensure that issues identified via testing are remediated according to the severity of the identified issue (e.g. remedy critical issues immediately or as soon as practicably possible within 30 days, remedy high severity issues within 30 days from when a patch is released from the applicable vendor, etc.). The testing under this **Section 2.7** shall include: (1) security application penetration testing conducted at least annually using data security/privacy industry standards to probe and test all external facing network and operating system elements that exist between the end-user and the application layer; and (2) vulnerability scans conducted at least quarterly using data security/privacy industry standards to test all internal systems and devices to identify vulnerabilities and remediate appropriate risks. Vendor agrees to ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit data as part of the Services, and establish a process for linking all access to such systems and applications. The Vendor agrees to ensure that security policies and procedures are in place to monitor and review security logs on a daily or weekly basis; and agrees that follow-up to exceptions found during such reviews will remediate those exceptions in a commercially reasonable manner. Vendor also agrees to use current industry best and commercially reasonable practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Vendor’s systems and networks or which provide access to Customer data. At least on an annual basis, at Customer’s request, Vendor shall provide Customer with copies of the reports based on the tests required under this **Section 2.7** as well as documentation proving Vendor’s compliance with this **Section 2.7**, such as documents demonstrating remediation.
8. Mobile Technology. In connection with the Services, Vendor agrees that if mobile applications are used to access data, then the mobile application shall be hosted within a secure container that is separate from any personal applications and data. The parties agree that under no circumstances is the data to be exchanged between secured and non-secured applications on a mobile device.
9. Cloud Technology. The parties agree that in regard to the development of cloud-based applications that will be used in conjunction with Vendor’s systems and/or Vendor’s data or Customer data, all such development must follow industry standard secure software development practices (such as OWASP and OWASP Mobile Security Project), wherein such practices include adhering to common controls and addressing top risks. The parties agree that when using cloud providers to access, transmit, store, or process data in connection with the services, they will ensure that appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations.
10. Notice of Security Incident. For purposes of this Exhibit, “Security Incident” shall mean an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the Information Security Program. Vendor shall notify Customer upon discovery of a Security Incident involving Vendor (or any of its respective subcontractors), as that Security Incident pertains to Customer’s data in accordance with the Business Associate Agreement. In the event of a reportable Security Incident, Vendor shall cooperate with investigations and provide all information reasonably requested by Customer, including without limitation: (i) the nature of the Security Incident; (ii) how Vendor identified the Security Incident; (iii) the anticipated impact to the PII or SPII; (iv) the Measures Vendor has implemented or plans to implement in order to prevent a recurrence of the Security Incident; and (v) any information required by law or statute (e.g., HIPAA).
11. **NOTICE OF LACK OF COMPLIANCE**

If Vendor discovers it has failed to comply with this Exhibit, Vendor shall, within five (5) days of discovery, disclose such failure to Customer in writing, together with a written remediation plan for achieving compliance. Vendor shall promptly notify Customer in the event that it can no longer comply with the Information Security Program described herein, whereupon Customer shall be entitled in its sole discretion to: (i) immediately terminate the Agreement; and/or (ii) require that all PII and/or SPII in Vendor’s (or its subcontractors) possession be deleted, destroyed, or returned to the notified party in accordance with the Agreement.

1. **MISCELLANEOUS**
2. Compliance Assessment. Customer may provide Vendor with a written request for certain information or access to Vendor’s premises, polices, books and records for purposes of assessing and monitoring Vendor’s compliance with its obligations under this Exhibit and Customer’s policies and procedures that relate to the use or disclosure of Customer data and the implementation of appropriate safeguards in relation to the Services provided. Within fifteen (15) days after such request, Vendor shall provide the requested information and access, cooperating with Customer in its assessment efforts. Customer shall bear the expenses of such assessment and shall use commercially reasonable efforts to conduct any on-site assessment in a manner so as not to unreasonably interfere with Vendor’s business activities. On an annual basis, at Customer’s request, Vendor shall complete a security questionnaire to certify that it has appropriate cyber and information security controls in place to safeguard and protect Customer data.
3. Governmental Audits. Vendor shall provide Customer with immediate written notice if any governmental entity requests a non-routine review, audit or other examination of the records or systems maintained by Vendor that support or contain Customer data. Vendor shall fully cooperate with Customer and governmental entities in connection with any such requests.
4. Minimum Service Levels. [Intentionally Omitted.]
5. Ownership. Except to the extent specifically provided in the Agreement: (i) the parties agree that Customer data (including all rights therein and related thereto) is and shall remain the sole and exclusive property of Customer, and no ownership or intellectual property rights to Customer data are granted to Vendor under this Exhibit; and (ii) any custom developed code and work products shall be owned by HEALTHeLINK.
6. Change Control Procedure. Should either party identify changes in scope, or should other matters arise, which would affect the current Agreement or statement of work, as applicable, the parties shall discuss the impact immediately, prior to any further work being performed. Furthermore, should either party identify any work that is not deemed appropriate under the Agreement or statement of work, if applicable, a new Agreement or statement of work, if applicable, shall be created for it.

**EXHIBIT G**

**Insurance Schedule**

1. VENDOR INSURANCE.

1.1 Types and Features. Pursuant to the Master Services Agreement (“Agreement”), Vendor shall maintain in full force and effect the following types of insurance at its sole expense to insure against risks of liability, in the minimum amounts set forth below (collectively, “Insurance Coverage”):

a) Commercial General Liability, in the minimum amount of $1,000,000 (one million dollars) per occurrence, $2,000,000 (two million dollars) aggregate, which includes a Personal & Advertising Injury Limit of $1,000,000 (one million dollars);

b) Cyber Liability Insurance in the minimum amount of $5,000,000 (five million dollars) per occurrence and $5,000,000 (five million dollars) in the aggregate, and including “Breach Response” sublimits of no less than $2,500,000 (2.5 million dollars).

c) Professional Liability Insurance (also known as “Errors and Omissions” coverage) in the minimum amount of $2,000,000 (two million dollars) per occurrence, $2,000,000 (two million dollars) aggregate; and

d) Worker’s Compensation insurance, with limits in compliance with applicable laws.

1.2 Copies To Be Provided. Vendor will provide HEALTHeLINK with copies of its insurance policies evidencing such coverage (or, if such insurance policies are not available, copies of its insurance binders or the best available evidence of such coverage) at HEALTHeLINK’s request.

2. HEALTHeLINK INSURANCE.

2.1 Coverage as Required Under the SHIN-NY. HEALTHeLINK will maintain Insurance Coverage in at least the minimum amounts required under the SHIN-NY.

2.2 Copies To Be Provided. HEALTHeLINK will provide Vendor with copies of its insurance policies evidencing such coverage (or, if such insurance policies are not available, copies of its insurance binders or the best available evidence of such coverage at Vendor’s request.

3. TERMS OF INSURANCE COVERAGE.

3.1 Terms of Policies. Each Party shall use its best commercially reasonable efforts to obtain, for each insurance policy required to be obtained and maintained pursuant to this Schedule, an agreement on the part of the issuing insurer that, in the event of cancellation of the policy in whole or in part, or a reduction as to coverage or amount thereof or other material change in the terms of the policy, whether initiated by the insurer or any insured, the insurer shall provide at least 30 days’ advance written notice to insured and to the other Party prior to such cancellation or reduction in coverage. With respect to any such insurance policy for which the issuing insurer does not agree to provide the aforementioned written notice to the other Party, the Party maintaining such Policy shall provide written notice to the other Party as soon as practicable upon receipt of notice of cancellation, reduction of coverage, or a material change in terms from the issuing insurer.

3.2 Primary Recovery. All insurance policies required to be carried by each Party shall be primary and any insurance maintained by the other Party is excess and noncontributory; provided, however, that this provision is intended to allocate responsibility for payment to the extent that policies issued to more than one Party may be required to respond to a covered event, and is not intended to relinquish or diminish any obligation of any insurance policy that is required to respond to such event. To the extent that this provision is deemed to have the latter effect if enforced, the Parties mutually intend that it not be given effect.

3.3 Waiver of Subrogation. Each Party agrees that it, its insurer(s) and anyone claiming by, through, under or on its behalf shall have no claim, right of action or right of subrogation against the other Party based on any loss or liability insured against or under the foregoing insurance; provided, however, that the Parties intend that this provision be enforced only to the extent that enforcement does not relinquish or diminish any rights of any Party to coverage under any of the insurance policies required to be obtained and maintained pursuant to this Schedule. Each Party shall use its best commercially reasonable efforts to obtain, for each such policy, au agreement on the part of the issuing insurer to include in the policy a waiver or subrogation provision consistent with this provision.

3.4 Claims-made Based Policies. If, in any of the foregoing cases, Vendor has procured a claims-made based policy (or policies) and such policy (or policies) are cancelled or not renewed, Vendor agrees to exercise any option contained in said policy (or policies) to extend the reporting period to the maximum period permitted; provided, however, that Vendor need not exercise such option if the superseding insurer will accept all prior claims.