DNA REGIMEN | WHITE-LABEL GENETIC TESTING SERVICES AGREEMENT

This White-Label Services Agreement (the "Agreement") is made and entered into as of _____ 2026 (the "Effective Date") by and between DNA Regimen, LLC ("DNA Regimen") with its principal place of business at 102 Scenic Drive, Georgetown, TX 78626, Suite 10101, and EC3Health ("Client" or "EC3Health ") with its principal place of business at 135 Jenkins St Ste 105B # 129, Saint Augustine, FL 32086 (individually a "Party" and collectively the "Parties").

RECITALS

WHEREAS, DNA Regimen owns and operates a proprietary precision-health solution known as "DNA Discovery," consisting of (i) a genetic test covering 123 clinically relevant single-nucleotide polymorphisms (SNPs) and (ii) tailored consultative insights guided by qualified genetic specialists (collectively, the "Services");

WHEREAS, Client desires to private-label and resell the Services to Client's end customers under Client's own branding and will assume responsibility for all front-end sales, billing, and initial customer communications, subject to the terms of this Agreement;

WHEREAS, DNA Regimen agrees to provide the Services on a white-label basis and to fulfill all back-end operational functions, including kit logistics, laboratory processing, report generation, and post-test consultations, under the terms and conditions set forth herein.

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

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party.

"Applicable Law" means all federal, state, and local statutes, regulations, and rules applicable to either Party or to the performance of this Agreement, including without limitation HIPAA, GINA, CLIA, FTC regulations, and Texas-specific genetic testing statutes.

"Customer" means an end user who purchases the Services from Client.

"Deliverables" means the DNA test kit, the completed genetic report, and any consultative findings delivered to a Customer.

"Confidential Information" has the meaning set forth in Section 7 below.

2. SERVICES PROVIDED BY DNA REGIMEN

2.1 **Kit Fulfillment & Logistics.** DNA Regimen shall (a) supply saliva-collection kits branded per Section 4, (b) ship kits to Customers, and (c) manage return-shipping logistics.

2.2 **Laboratory Testing.** DNA Regimen shall perform or subcontract CLIA-certified laboratory testing on received samples to analyze the 123 SNPs included in the DNA Discovery panel.

2.3 **Report Generation.** DNA Regimen shall prepare a personalized genetic insights report (the "Report") for each Customer based on the laboratory results.

2.4 **Consultation.** DNA Regimen shall provide each Customer with a one-on-one telehealth or telephonic consultation with a qualified genetic specialist to review the Report.

2.5 **Support Escalation.** DNA Regimen shall provide tier-2 technical and clinical support for issues escalated by Client under Section 3.3.

3. CLIENT RESPONSIBILITIES

3.1 **Branding, Marketing, and Sales.** Client shall promote and sell the Services under Client's trademarks at its own expense and in compliance with Applicable Law and Section 4.

3.2 **Payment Collection.** Client is solely responsible for collecting payments from Customers. DNA Regimen will invoice Client in accordance with Exhibit A (Pricing & Payment Terms).

3.3 **Customer Service.** Client shall provide first-level customer support, including but not limited to order inquiries, status updates, and non-clinical questions. Issues beyond Client's scope shall be escalated to DNA Regimen in accordance with mutually agreed procedures.

3.4 **Data Transmission.** Client shall transmit to DNA Regimen accurate Customer shipping information, consent forms, and any required health data using secure, encrypted channels.

3.5 **Compliance.** Client shall (a) obtain all legally required consents, authorizations, and notices from Customers, (b) disclose DNA Regimen's involvement as a subcontracted clinical service provider if and as required by law, and (c) comply with all Applicable Law.

4. BRANDING AND WHITE-LABEL REQUIREMENTS

4.1 **White-Label Branding.** Except as otherwise required by law, the Deliverables may bear Client's branding, provided that DNA Regimen's name appears in professional or regulatory disclosures (e.g., "Laboratory services performed by DNA Regimen, LLC, a CLIA-certified lab").

4.2 **Use of Marks.** Each Party grants to the other a limited, non-exclusive, non-transferable, royalty-free license during the Term to use its trademarks solely as necessary to fulfill the objectives of this Agreement and in accordance with the owner's trademark guidelines.

4.3 **No Co-Branding Without Approval.** Neither Party shall use the other Party's marks in press releases or promotional materials without prior written approval.

5. COMPLIANCE WITH LAWS; DATA PRIVACY & SECURITY

5.1 **HIPAA & PHI.** To the extent DNA Regimen receives protected health information ("PHI"), DNA Regimen shall act as a Business Associate and the Parties shall execute a Business Associate Agreement ("BAA"), attached as Exhibit B.

5.2 **Privacy.** Each Party shall implement and maintain industry-standard administrative, technical, and physical safeguards to protect Customer data and comply with all privacy, data-protection, and genetic-testing laws.

5.3 **De-Identification & Research.** DNA Regimen may use anonymized and de-identified data for quality assurance, internal research, and product development, provided such use complies with Applicable Law.

6. INTELLECTUAL PROPERTY

6.1 **Ownership.** All intellectual property rights in the DNA Discovery platform, test methodology, algorithms, reports, and related know-how are and shall remain the exclusive property of DNA Regimen.

6.2 **Client Content.** Client retains ownership of its trademarks, marketing materials, and customer lists.

6.3 **License to Deliverables.** DNA Regimen grants Client a non-exclusive, non-transferable license to distribute the Deliverables to Customers in accordance with this Agreement.

7. CONFIDENTIALITY

7.1 **Definition.** "Confidential Information" means all non-public information disclosed by one Party to the other, whether oral or written, that is designated as confidential or that a reasonable person would understand to be confidential.

7.2 **Obligations.** The receiving Party shall (a) use Confidential Information only for the purposes of this Agreement, (b) protect it with the same degree of care it uses for its own confidential information (and at least reasonable care), and (c) disclose it only to employees and contractors with a need to know who are bound by similar obligations.

7.3 **Exclusions.** Confidential Information does not include information that is publicly available, already known, independently developed without reference to the disclosing Party's information, or rightfully obtained from third parties without obligation of confidentiality.

7.4 **Compelled Disclosure.** The receiving Party may disclose Confidential Information if required by law, provided it gives prompt notice to the disclosing Party and cooperates in seeking protective measures.

8. REPRESENTATIONS & WARRANTIES; DISCLAIMERS

8.1 **Mutual Warranties.** Each Party represents that it is duly organized, in good standing, and has full authority to enter into this Agreement.

8.2 **DNA Regimen Warranties.** DNA Regimen warrants that (a) its laboratory operations are CLIA-certified and compliant with Applicable Law, and (b) Services shall be performed in a professional and workmanlike manner.

8.3 **Client Warranties.** Client warrants that it will market and sell the Services truthfully and in compliance with Applicable Law.

8.4 **DISCLAIMER.** EXCEPT AS EXPRESSLY PROVIDED, DNA REGIMEN DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. REPORTS AND CONSULTS ARE PROVIDED FOR EDUCATIONAL PURPOSES AND ARE NOT A DIAGNOSTIC TOOL OR MEDICAL ADVICE.

9. INDEMNIFICATION

9.1 **By DNA Regimen.** DNA Regimen shall indemnify, defend, and hold Client harmless from third-party claims arising from (a) DNA Regimen's breach of this Agreement, (b) negligence or willful misconduct, or (c) infringement of third-party IP rights by the Services.

9.2 **By Client.** Client shall indemnify, defend, and hold DNA Regimen harmless from third-party claims arising from (a) Client's breach of this Agreement, (b) Client's marketing or resale of the Services, or (c) Client's negligence or willful misconduct.

9.3 **Procedure.** The indemnified Party shall promptly notify the indemnifying Party of any claim, allow control of the defense, and cooperate at the indemnifying Party's expense.

10. LIMITATION OF LIABILITY

EXCEPT FOR A PARTY'S INDEMNIFICATION OBLIGATIONS OR BREACH OF CONFIDENTIALITY, IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR (A) INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, OR (B) AGGREGATE DAMAGES IN EXCESS OF THE FEES PAID OR PAYABLE TO DNA REGIMEN UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO LIABILITY.

11. INSURANCE

Each Party shall maintain, at its own expense, commercially reasonable levels of general liability, professional liability, and cyber liability insurance, and shall provide certificates of insurance upon request.

12. TERM & TERMINATION

12.1 **Term.** This Agreement commences on the Effective Date and continues in perpetuity until/unless terminated in accordance with Sections 12.2 and 12.3. .

12.2 **Termination for Convenience.** Either Party may terminate this Agreement for any reason upon sixty (60) days' prior written notice.

12.3 **Termination for Cause.** Either Party may terminate immediately for (a) material breach not cured within thirty (30) days of notice, (b) bankruptcy or insolvency, or (c) change in law rendering performance illegal.

13. EFFECTS OF TERMINATION

Upon termination, (a) Client shall cease marketing the Services, (b) outstanding orders shall be completed or canceled by mutual agreement, (c) each Party shall return or destroy the other's Confidential Information, and (d) Sections 6–11, 13, 14, and 15 shall survive.

14. DISPUTE RESOLUTION; ARBITRATION

14.1 **Informal Resolution.** The Parties shall first attempt in good faith to resolve any dispute through negotiations between executives.

14.2 **Binding Arbitration.** If unresolved within thirty (30) days, disputes shall be finally settled by binding arbitration administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules. The seat of arbitration shall be Austin, Texas, and judgment on the award may be entered in any court of competent jurisdiction.

15. GOVERNING LAW; VENUE

This Agreement and any disputes arising hereunder shall be governed by and construed in accordance with the laws of the State of Texas, without regard to its conflict-of-law principles. The Parties irrevocably submit to arbitration in Texas as set forth in Section 14.

16. MISCELLANEOUS

16.1 **Independent Contractors.** The Parties are independent contractors; nothing herein creates a partnership, joint venture, or agency relationship.

16.2 **Assignment.** Neither Party may assign this Agreement without the other Party's prior written consent, except to an Affiliate or successor in interest to substantially all assets.

16.3 **Force Majeure.** Neither Party shall be liable for delays due to causes beyond its reasonable control.

16.4 **Notices.** Notices shall be in writing and deemed given when delivered by certified mail, courier, or email with confirmation, to the addresses set forth above.

16.5 **Entire Agreement; Amendment.** This Agreement (including Exhibits) constitutes the entire agreement between the Parties and supersedes all prior agreements. No amendment shall be effective unless in writing and signed by both Parties.

16.6 **Severability; Waiver.** If any provision is held invalid, the remainder shall remain in force. Failure to enforce any provision shall not constitute waiver.

16.7 **Non-Circumvention**. Each Party (the "Receiving Party") acknowledges that the other Party (the "Disclosing Party") has expended substantial effort and resources in developing and maintaining its respective laboratory network, specialist panels, customers, suppliers, and other strategic business relationships (collectively, "Protected Relationships"). Accordingly, during the Term and for three (3) years following termination or expiration of this Agreement, neither Party shall, directly or indirectly, solicit, contract with, engage, or otherwise circumvent the other Party to obtain or provide services that are identical or materially similar to those contemplated under this Agreement from or to (a) any Protected Relationship of the Disclosing Party, or (b) any Customer or prospective customer introduced to the Receiving Party by the Disclosing Party, without the Disclosing Party's prior written consent. Any violation of this Section 16.8 shall constitute a material breach of this Agreement, and the non-breaching Party

shall be entitled to seek injunctive relief (without the necessity of posting bond) and any other remedies available at law or in equity. This Section 16.8 shall survive termination of this Agreement.

16.8 **Counterparts; Electronic Signatures.** This Agreement may be executed in counterparts, including electronically, each of which is deemed an original and together constitute one instrument. **[END TERMS] [SIGNATURE PAGE FOLLOWS] [REMAINDER OF PAGE LEFT BLANK]**

SIGNATURES

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date.

DNA Regimen, LLC	**EC3Health**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

[END AGREEMENT] [EXHIBIT A FOLLOWS] [REMAINDER OF PAGE LEFT BLANK]

EXHIBIT A – PRICING & PAYMENT TERMS

Services	Client Price (wholesale)	Provider Price	Revenue to Client
DNA Discovery: DNA collection kit, shipping, lab services, reporting, AI consult	$299	$399	$100
PGx Complete: Comprehensive and Validated PGx	$199	$249	$50
DNA Discovery Clinical: Bundled NGx and PGx	$469	$619	$150

Payment Terms

Client shall act as the merchant of record and shall be solely responsible for processing customer payments and managing any associated risks, including chargebacks. The Parties shall utilize Stripe, Inc. (“Stripe”) or a mutually agreed-upon payment processor to facilitate payment processing.

Client shall remit to DNA Regimen payment (“Payment”) at the time of each customer transaction. DNA Regimen shall have no obligation to fulfill any order unless and until the corresponding Payment has been received in full.

In the event of a chargeback or other reversal of funds related to an order previously fulfilled by DNA Regimen, Client shall have the right to recover the amount of such chargeback from DNA Regimen. Client may offset such amounts against future payments due to DNA Regimen or, if no such payments are due, may invoice DNA Regimen for the chargeback amount, which DNA Regimen shall remit within fifteen (15) days of receipt. **[END EXHIBIT A] [REMAINDER OF PAGE LEFT BLANK] [EXHIBIT B FOLLOWS]**

Business Associate Agreement

This Business Associate Agreement (this “BAA” or “Agreement”) is an Exhibit to and made part of the underlying services agreement (the “Underlying Agreement”) between EC3Health (“EC3Health ”), and DNA Regimen, LLC, a Business Associate (“Business Associate”). This BAA is effective as of the Effective Date of the Underlying Agreement. The Parties hereby agree to the following terms, which are intended to ensure full compliance with the Health Insurance Portability and Accountability Act of 1996 and its regulations (“HIPAA”), as well as applicable state privacy laws, regarding the handling of Protected Health Information.

Background and Purpose

Role of Covered Entity. EC3Health is not a Covered Entity under HIPAA, but they do contract with Covered Entities that provide certain health-related services. EC3Health collects only basic personally identifiable information (“PII”) and payment information from individuals at the point of sale, but does not collect or maintain any Protected Health Information (PHI) prior to or during the sale of any services. EC3Health's involvement in patient health data is limited to directing individuals to the Business Associate’s platform post-sale.

Role of Business Associate. DNA Regimen, LLC operates a white-labeled platform on behalf of EC3Health to deliver genetic testing and related services to individuals. After completing a purchase with EC3Health , customers are routed to DNA Regimen’s platform where all health-related data and PHI are collected from the individual and processed by DNA Regimen. In performing these services, DNA Regimen is functioning as a “Business Associate” to EC3Health as defined by HIPAA.

PHI Collected and Processed. The PHI created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity includes genetic information and test results, laboratory results, and any other individually identifiable health information provided by individuals through the DNA Regimen platform. Such information is considered PHI under HIPAA. Business Associate acknowledges that it will have access to and will process this PHI solely to perform the services for EC3Health as described in the Underlying Agreement.

Patient Consent Responsibilities. Business Associate is solely responsible for obtaining any necessary patient consents or authorizations for the collection, use, and disclosure of PHI via its platform. This includes, without limitation, obtaining any specific written consents required by applicable state laws for genetic information and test data. Business Associate shall ensure that individuals are provided with all required notices and disclosures and that any sharing of PHI is done only with proper consent or as otherwise permitted by law.

Need for BAA. EC3Health and DNA Regimen desire to formally outline their obligations with respect to PHI privacy and security. This BAA is intended to include all required elements under HIPAA and HITECH, and to establish each Party’s responsibilities in safeguarding PHI. It also

addresses state-specific privacy and security laws to the extent they apply to the information handled, in order to provide comprehensive protection of individual data.

NOW, THEREFORE, in consideration of the mutual promises and covenants herein, and for other good and valuable consideration, the sufficiency of which is acknowledged, the Parties agree as follows.

1. Definitions

For purposes of this BAA, the following terms shall have the meanings set forth below. Capitalized terms used but not otherwise defined in this Agreement shall have the definitions set forth in HIPAA and its implementing regulations.

Covered Entity. "Covered Entity" shall generally have the same meaning as at 45 C.F.R. § 160.103, and in this Agreement refers specifically to EC3Health and/or to any parties engaged with EC3Health for the purposes of fulfilling services provided by . Covered Entity is the entity on whose behalf the Business Associate handles PHI.

Business Associate. "Business Associate" shall have the meaning given at 45 C.F.R. § 160.103. In this Agreement, Business Associate refers specifically to DNA Regimen, LLC. Business Associate is the entity performing services involving PHI on behalf of the Covered Entity.

Protected Health Information (PHI). "Protected Health Information" or "PHI" means individually identifiable health information that is transmitted or maintained in any form or medium, as defined at 45 C.F.R. § 160.103, limited to the information Business Associate creates, receives, maintains, or transmits on behalf of EC3Health under the Underlying Agreement. For purposes of this BAA, PHI includes genetic information and lab test results provided by individuals via the Business Associate's platform, and any other health information linked to an individual that Business Associate handles on EC3Health behalf. PHI does not include de-identified information as defined by 45 C.F.R. § 164.514(b).

Electronic Protected Health Information (ePHI). "Electronic PHI" or "ePHI" means PHI that is transmitted or maintained in electronic media. All obligations in this Agreement applicable to PHI apply equally to ePHI, and Business Associate specifically acknowledges its obligation to protect ePHI in compliance with the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C).

Genetic Information. "Genetic Information" means information about an individual's genetic tests and the genetic tests of an individual's family members, as well as any manifestation of a disease or disorder in family members, as defined in 45 C.F.R. § 160.103. Genetic Information is considered PHI under HIPAA when it is individually identifiable. For purposes of this Agreement, any Genetic Information collected or processed by Business Associate is PHI and subject to all the same protections.

Personal Information. “Personal Information” (or “PI”) means any information that identifies, relates to, describes, or is reasonably capable of being associated with an individual, in accordance with applicable privacy laws, excluding any information that is considered PHI. (For example, the basic contact and payment information collected by Covered Entity at point-of-sale may be Personal Information but not PHI.) Personal Information is mentioned in this BAA in the context of state privacy laws (such as the CCPA) that may apply to such data if not covered by HIPAA.

Applicable Law. “Applicable Law” means all federal and state laws and regulations that apply to the Parties or the subject matter of this Agreement, including but not limited to HIPAA, the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”), the regulations promulgated under HIPAA and HITECH (including the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164), and applicable state data privacy and security laws such as the California Consumer Privacy Act (“CCPA”), as amended, the New York SHIELD Act, and any state genetic privacy laws or other health information privacy laws that impose requirements more stringent than HIPAA. In the event of a conflict between HIPAA and a state law, the more stringent provision shall generally control, consistent with 45 C.F.R. § 160.203.

Breach. “Breach” means the unauthorized acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the HIPAA Privacy Rule, which compromises the security or privacy of the PHI, as defined in 45 C.F.R. § 164.402. “Unsecured PHI” is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS.

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

Services. “Services” means the services provided by Business Associate to Covered Entity as described in the Underlying Agreement. In summary, these include providing a platform and related services for genetic testing and analysis for individuals referred by Covered Entity, which involve the collection and processing of PHI. This BAA governs how PHI may be used or disclosed in the course of providing the Services.

2. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement or by Applicable Law, Business Associate is permitted to use and disclose PHI that it creates or receives on behalf of EC3Health only as follows.

- **2.1 Provision of Services (Primary Purpose)**. Business Associate may use and disclose PHI solely for the purpose of providing the Services to or on behalf of Covered Entity as set forth in the Underlying Agreement. This includes using PHI for Business Associate’s performance of genetic testing and analysis, reporting results to the

individuals and/or to any Covered Entity if required, facilitating consultations, and any related health care operations of any Covered Entity that Business Associate has been engaged to perform. All such uses and disclosures of PHI must be limited to the minimum necessary to accomplish the intended purpose, in accordance with 45 C.F.R. § 164.502(b). A Covered Entity will not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity itself except as specifically permitted for Business Associate's management and administration as elsewhere provided for in this Agreement.

- **2.2 Internal Management and Legal Responsibilities**. Business Associate may use PHI for its proper management and administration or to carry out its legal responsibilities, and may disclose PHI for such purposes only if.

  (a) the disclosure is required by law, or

  (b) Business Associate obtains reasonable written assurances via a confidentiality agreement from the third party receiving the PHI that the information will be kept confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed, and the third party agrees to notify Business Associate of any instances of which it becomes aware that the confidentiality of the PHI has been breached per 45 C.F.R. § 164.504(e)(4). Examples of uses or disclosures under this subsection include. disclosures to Business Associate's professional advisors for legal advice or auditing, or disclosures to regulatory authorities if required by law.

- **2.3 Data Aggregation Services**. If requested or permitted by EC3Health , Business Associate is authorized to perform data aggregation services. "Data aggregation" means the combining of PHI by Business Associate with PHI from other covered entity clients of Business Associate, to permit data analyses that relate to the provision of services by EC3Health . Any data aggregation involving PHI from multiple sources will be used or disclosed only for EC3Health's purposes, and not for any unrelated purpose. Business Associate shall ensure that any data aggregation use/disclosure is appropriately authorized under this BAA and Applicable Law.

- **2.4 De-Identification of PHI**. Business Associate may de-identify PHI in its possession only if and to the extent that de-identification is

  (a) performed in compliance with 45 C.F.R. § 164.514(b) (the HIPAA de-identification standard), and

  (b) permitted under the Underlying Agreement or otherwise expressly authorized in writing by Covered Entity. De-identified data is not considered PHI and may be used or disclosed by Business Associate for permissible purposes in accordance with the Underlying Agreement and Applicable Law. However, Business

Associate may not attempt to re-identify any de-identified data nor permit any third party to do so.

- **2.5 No Other Use or Disclosure**. Business Associate shall not use or further disclose PHI other than as permitted or required by this Agreement or as required by law per 45 C.F.R. § 164.103. Business Associate is expressly prohibited from using or disclosing PHI for any purpose that would violate HIPAA's Privacy Rule if done by EC3Health including, but not limited to, any use of PHI for marketing or sale of PHI without the individual's authorization, or any use of genetic information for underwriting purposes.

3. Duties and Obligations of Business Associate

Business Associate hereby agrees to comply with the following obligations, which are intended to satisfy the requirements of 45 C.F.R. § 164.504(e) and other applicable provisions of HIPAA and HITECH for business associate agreements, as well as to incorporate industry best practices for security and privacy.

- **3.1 Compliance with Privacy Rule Requirements**. To the extent Business Associate is carrying out any obligation of EC3Health under the HIPAA Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation per 45 C.F.R. § 164.504(e)(2)(ii)(H). For example, if and as directed by EC3Health , Business Associate will provide necessary information to assist EC3Health in drafting any required notices or responding to requests from individuals to exercise their privacy rights. Business Associate will not engage in any act or practice that would violate the Privacy Rule if done by the EC3Health .

- **3.2 Safeguards for PHI**. Business Associate shall use appropriate safeguards to prevent any use or disclosure of PHI other than as permitted by this Agreement. This includes implementing and maintaining administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic PHI that Business Associate creates, receives, maintains, or transmits on behalf of EC3Health , as required by the HIPAA Security Rule (45 C.F.R. §§ 164.308, 164.310, 164.312). At minimum, Business Associate's safeguards shall include.

  (a) access controls to ensure only authorized personnel can access PHI;

  (b) encryption of PHI stored on electronic systems and in transit, in line with industry standards (e.g., using encryption methods meeting HHS guidance for rendering PHI unusable/unreadable);

  (c) workforce training on privacy and security obligations;

(d) policies and procedures for identifying and mitigating potential security risks; and

(e) other reasonable measures to protect against anticipated threats or hazards. Business Associate shall regularly assess and update its safeguards to ensure ongoing protection of PHI in compliance with HIPAA and any more stringent state data security requirements. (For example, compliance with HIPAA's Security Rule generally satisfies the data security program requirements of New York's SHIELD Act, but Business Associate shall ensure any additional measures needed under state law for the particular types of data – such as genetic data – are also implemented.)

- **3.3 Subcontractors and Agents**. Business Associate shall ensure that any subcontractors or agents to whom it provides PHI (or who create, receive, maintain, or transmit PHI on behalf of Business Associate) agree in writing to the same restrictions, conditions, and requirements that apply to Business Associate under this BAA. In particular, before any subcontractor is granted access to PHI, Business Associate will enter into a written agreement with that subcontractor that.

  (a) imposes at least the same obligations to protect PHI as are imposed on Business Associate in this Agreement; and

  (b) if applicable, designates the subcontractor as a business associate under HIPAA. Business Associate remains fully responsible for any acts or omissions of its subcontractors or agents in the handling of PHI, and shall monitor and audit, as reasonably necessary, each subcontractor's performance to ensure compliance with privacy and security obligations.

- **3.4 Prohibition on Unauthorized Uses/Disclosures**. Business Associate shall not use or further disclose PHI other than as permitted or required by this Agreement or as required by law. If Business Associate is ever in doubt whether a proposed use or disclosure is permitted, it will refrain from the activity and consult with EC3Health to obtain clarification or necessary authorization. Business Associate acknowledges that unauthorized uses or disclosures of PHI are grounds for Covered Entity to terminate this Agreement and the Underlying Agreement for cause pursuant to Section 8.2 herein.

- **3.5 Mitigation.** In the event of any unauthorized use or disclosure of PHI by Business Associate or its agents, Business Associate shall immediately act to mitigate, to the extent practicable, any harmful effect of such use or disclosure. This may include retrieving improperly disclosed information, providing credit monitoring or identity theft protection services if financial information was involved, or other reasonable mitigation steps. Business Associate shall bear the costs of mitigation to the extent the incident was caused by its breach of this Agreement or its negligence or willful misconduct. Business Associate shall also cooperate with EC3Health in mitigating any harmful effects, including by coordinating communications with affected individuals or regulators

as appropriate.

- **3.6 Disclosure Accounting**. Business Associate agrees to document all disclosures of PHI and information related to such disclosures as would be required for EC3Health to respond to an individual's request for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. This includes tracking any disclosures that Business Associate makes to third parties other than those excepted from accounting under HIPAA, such as disclosures for treatment, payment, or health care operations. Upon request, Business Associate shall provide to EC3Health the information necessary for EC3Health to provide an accounting of disclosures to an individual, as required by 45 C.F.R. § 164.528. Such information shall be provided in an electronic spreadsheet or other format reasonably specified by EC3Health , and within a reasonable time after request. These obligations for accounting of disclosures shall survive termination of the Agreement for so long as Business Associate maintains the PHI.

- **3.7 Access to PHI**. If Business Associate maintains PHI in a Designated Record Set (as defined in 45 C.F.R. § 164.501) for EC3Health , Business Associate shall make such PHI available to EC3Health or, at EC3Health's direction, directly to the individual who is the subject of the PHI in order to satisfy EC3Health's legal obligations. This means that, upon EC3Health's request, Business Associate will provide access to the requested PHI in the format requested if it is readily producible in that format, or if not, in a mutually agreeable format. Business Associate shall provide such access in a timely manner, not later than 15 days after receiving a request from EC3Health (or such shorter time as may be required by applicable state law). If an individual makes a request for access directly to Business Associate, Business Associate shall forward that request to EC3Health within 5 business days, and shall not provide access directly to the individual unless directed by EC3Health or where required by law.

- **3.8 Amendment of PHI**. If Business Associate maintains PHI in a Designated Record Set, it shall accommodate any requests from EC3Health or from any customer directly to amend the PHI pursuant to 45 C.F.R. § 164.526. Upon receipt of a written request from EC3Health or from any customer directly to amend PHI, Business Associate shall promptly incorporate any amendments, additions, or corrections to the PHI as directed. If an individual sends a request for amendment directly to Business Associate, Business Associate shall forward it to EC3Health within 5 business days of receipt. Any denial of a requested amendment remains the responsibility of EC3Health ; however, Business Associate shall reasonably cooperate in providing the necessary information to prepare such a denial if needed.

- **3.9 Availability of Books and Records**. Business Associate agrees to make its records relating to the use and disclosure of PHI received from, or created or received on behalf of, EC3Health available to the Secretary of the U.S. Department of Health and Human Services (HHS) for purposes of determining compliance with HIPAA. Business Associate shall promptly notify EC3Health if it receives such a request from HHS, and shall provide

EC3Health with a copy of any materials furnished, unless prohibited by law. Additionally, Business Associate shall reasonably cooperate with EC3Health in any requests for information or documentation from state regulators with jurisdiction regarding PHI handling, to the extent such information is requested to evaluate compliance with privacy or security laws.

3.10 Obtaining Consents and Authorizations. As noted in the Background, Business Associate is responsible for obtaining all necessary individual consents or authorizations for the collection, use, and disclosure of PHI via the DNA Regimen platform. Business Associate shall ensure that its processes and forms for obtaining consent or authorization comply with all applicable laws. This includes, without limitation:

(a) **HIPAA Authorization (if needed)**. If any use or disclosure of PHI that Business Associate wishes to make (or is instructed to make) falls outside the scope of Treatment, Payment, or Health Care Operations (as defined by HIPAA) or otherwise is not permitted by the Privacy Rule without an individual's authorization, Business Associate must obtain a valid HIPAA-compliant Authorization from the individual before such use/disclosure. For example, if Business Associate were to use PHI for its own marketing purposes or to disclose PHI to a third party for marketing, an authorization would be required. Business Associate shall not solicit or use any authorizations for uses/disclosures not permitted by EC3Health .

(b) **State Genetic Privacy Consents**. Business Associate shall obtain any specific written consents required by state laws for genetic information. Business Associate will identify and comply with any such laws in the jurisdictions where individuals using the platform reside. This may include, for instance, obtaining a standalone consent for DNA sample collection and analysis, as required by laws like the Alaska Genetic Privacy Act or similar statutes in other states, and ensuring individuals are informed about how their genetic data will be used and shared.

(c) **Consent for Data Sharing**. To the extent Business Associate will share PHI with any third parties, Business Associate must ensure it has obtained the individual's consent or authorization as required by law. Business Associate must also limit such sharing to what was consented to and provide individuals with any required rights.

3.11 Minimum Necessary Standard. In performing its functions and using or disclosing PHI as permitted by this Agreement, Business Associate shall adhere to the "minimum necessary" standard. This means Business Associate shall access, use, and disclose only the minimum PHI necessary to accomplish the intended purpose of the use or disclosure, in compliance with 45 C.F.R. § 164.502(b). Business Associate shall impose similar minimum necessary restrictions on its subcontractors and workforce. When requesting PHI from EC3Health or another source, Business Associate shall request only the minimum necessary information needed for the task.

3.12 Reporting of Improper Use or Disclosure. Business Associate shall report to EC3Health without unreasonable delay any use or disclosure of PHI not provided for by this Agreement of which it becomes aware. Specifically, Business Associate will notify EC3Health in writing of:

(a) any unauthorized access, use, or disclosure of PHI within five (5) calendar days of discovering such incident; and

(b) any Breach of Unsecured PHI without unreasonable delay and in no case later than five (5) calendar days after discovery of the Breach. Such report shall include, to the extent known, the identification of each individual whose PHI was or is reasonably believed to have been accessed, acquired, or disclosed during the incident, and other available information that EC3Health is required to include in a breach notification. Business Associate shall supplement the report with additional information as it becomes available. In the event of a Breach, Business Associate's notice to EC3Health shall also include, where known, the root cause of the incident and the corrective actions Business Associate has undertaken or plans to undertake to mitigate and prevent further incidents.

- **3.13 Breach Notification Cooperation**. In addition to the reporting obligations above, Business Associate shall cooperate with EC3Health in the breach notification process. EC3Health has the responsibility under HIPAA to notify affected individuals, HHS, and potentially the media of a Breach of unsecured PHI without unreasonable delay and within sixty (60) days of discovery. Business Associate shall assist EC3Health by providing any requested information and supporting investigation of the breach. If the breach triggers notification obligations under state laws, Business Associate shall also assist EC3Health in meeting those requirements. Notably, if the breach involves residents of certain states like California or New York, additional notifications may be required. Business Associate will provide information necessary for EC3Health to comply with such state-specific obligations. Business Associate shall not notify any individuals or third parties of a Breach without EC3Health's prior written consent, unless required by law.

- **3.14 Audit Rights**. Business Associate agrees that EC3Health shall have the right to conduct reasonable periodic audits of Business Associate's operations to verify compliance with this BAA and applicable law. Such audits may include a review of security measures and policies, and interviews of relevant personnel. EC3Health shall give reasonable prior written notice and conduct audits during normal business hours, and both parties shall cooperate in good faith to minimize disruption. Business Associate shall promptly address any findings or vulnerabilities identified by such an audit, including implementing any corrective actions reasonably requested by EC3Health . In addition to EC3Health initiated audits, Business Associate shall undergo any third-party security assessments as may be required under the Underlying Agreement (e.g., if a certain standard or certification is mandated) and provide EC3Health with summaries of those results upon request, to the extent they relate to the PHI protection. Nothing in this

section shall limit HHS's or any regulator's ability to audit Business Associate as provided by law, and Business Associate's obligation to allow such audit per Section 3.9.

3.15 Security Incidents (Non-Breach). Business Associate shall report to EC3Health , upon request, a summary of any Security Incidents that do not constitute a Breach, on a reasonable basis. The Parties acknowledge that this subsection is intended to address routine or insignificant matters that occur in the normal course of business and do not result in any unauthorized access to PHI. Business Associate shall document and keep records of such incidents in accordance with its own risk management policies and make those records available to EC3Health upon reasonable request, to demonstrate Business Associate's efforts in monitoring and responding to security events.

4. Obligations of EC3Health

Covered Entity agrees to.

- **4.1 Provision of Privacy Practices and Restrictions**. Notify Business Associate of any limitations in EC3Health's Notice of Privacy Practices to the extent that such limitations may affect Business Associate's use or disclosure of PHI. EC3Health will also inform Business Associate of any changes in, or revocation of, permission by an individual to use or disclose PHI, if such changes affect Business Associate's permitted uses or disclosures. Further, EC3Health shall notify Business Associate of any confidential communications requests or restrictions on the use/disclosure of PHI that EC3Health has agreed to, to the extent that such restriction may affect Business Associate's activities. Business Associate shall then accommodate any such agreed restrictions, provided that EC3Health notifies Business Associate in writing of the restriction.

4.2 Minimum Necessary Information. Disclose or permit access to Business Associate only the minimum necessary PHI for Business Associate to perform the Services. EC3Health will refrain from affirmatively providing Business Associate with any PHI that is not needed for Business Associate's duties.

4.3 No Impermissible Requests. EC3Health will not ask Business Associate to use or disclose PHI in a manner that would not be permissible under HIPAA if done by EC3Health , except that Business Associate may use or disclose PHI for its proper management and administration or legal responsibilities as set forth in Section 2.2 above. EC3Health understands and agrees that it must not direct or pressure Business Associate to engage in any activity that would violate any Applicable Law or the terms of this BAA.

4.4 Obtain Any Required Consents. To the extent EC3Health has any role in obtaining consent or authorization from individuals, EC3Health shall ensure that such consents or notices are in place. The Parties acknowledge that Business Associate is primarily responsible for obtaining patient consent for genetic data as described in Section 3.10. EC3Health's obligation is to support or not contradict those consent processes. EC3Health will cooperate with Business

Associate by, for instance, informing individuals at point-of-sale that they will be redirected to a third-party platform (DNA Regimen) which will collect their health information, so the individual is aware and can make an informed choice to proceed.

4.5 Monitoring and Compliance.EC3Health shall monitor the services provided by Business Associate as it deems appropriate to ensure compliance with this Agreement. If EC3Health becomes aware of a pattern of activity or practice of Business Associate that constitutes a material breach or violation of Business Associate's obligations under this BAA, EC3Health will notify Business Associate and provide an opportunity for Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within a reasonable time specified by EC3Health shall have the right to terminate this Agreement and the Underlying Agreement, if feasible, in accordance with Section 8.2.

4.6 Safeguarding of PII. Although EC3Health does not collect and share PHI with Business Associate, it does collect and maintain certain Personal Information (PII) at the point of sale. EC3Health agrees that it will implement reasonable and appropriate safeguards to protect the security of such PII in its possession. To the extent any Personal Information collected by EC3Health is later shared with Business Associate, EC3Health will comply with any applicable privacy law before transferring such data. EC3Health will not provide Business Associate with any information that the individual has not agreed to share or that EC3Health is not authorized to share under applicable law.

5. Compliance with State Privacy Laws.

The Parties acknowledge that, in addition to HIPAA, certain state privacy and data security laws may apply to the information and activities covered by this Agreement. Recognizing the sensitivity of genetic information, the Parties acknowledge that certain states impose heightened protections for genetic data. Business Associate shall ensure compliance with any such laws in the jurisdictions where Services are offered. This includes, without limitation, laws that require written informed consent for the collection or disclosure of genetic information, or that restrict the use of genetic data (for example, prohibiting disclosure of identifiable genetic info to third parties like insurers or employers without consent). Business Associate will obtain any required consent from individuals and will limit its use and disclosure of genetic information strictly to what is permitted by those individuals and by law. EC3Health shall reasonably assist or cooperate with Business Associate by providing any information it has about an individual's preferences or restrictions concerning their genetic data, if such information comes to EC3Health's attention. Both Parties will also comply with the federal Genetic Information Nondiscrimination Act (GINA) to the extent applicable (noting that GINA mainly restricts insurers and employers in the use of genetic info, but it underscores the importance of keeping genetic PHI confidential and not using it improperly).

The Parties agree to monitor and comply with other applicable state privacy laws such as the Illinois Genetic Information Privacy Act, the California Confidentiality of Medical Information Act (CMIA), Florida's Patient Data Privacy laws, Texas Medical Privacy Act, or any successor or

new laws like the Virginia Consumer Data Protection Act (CDPA), etc., to the extent they apply to the operations under this Agreement. Where a state law regarding health information imposes more restrictive requirements than HIPAA, the Parties shall treat those requirements as binding. Business Associate will promptly alert EC3Health if it believes that a specific state law applies that would affect the permissible use or disclosure of PHI or Personal Information or would necessitate changes to the Services or practices. The Parties will then confer in good faith to make any necessary modifications to ensure compliance.

6. Term and Termination

6.1 Term. This BAA shall commence on the Effective Date stated above and shall remain in effect until the Underlying Agreement is terminated or expires, and thereafter until all PHI in the possession of Business Associate or its subcontractors is either returned to EC3Health or destroyed in accordance with Section 6.3. This Agreement may be terminated earlier if mutually agreed in writing by the Parties or if terminated for cause as described below.

6.2 Termination for Cause. EC3Health may immediately terminate this BAA (and any related Underlying Agreement, if it so elects) if EC3Health determines that Business Associate has engaged in a material breach or violation of this BAA. Alternatively, at EC3Health's option, EC3Health may provide written notice of the breach and give Business Associate an opportunity to cure the breach or end the violation within a time specified (not to exceed 30 days). If Business Associate does not cure the breach or end the violation within the specified time, EC3Health may terminate this Agreement and the Underlying Agreement.

6.3 Disposition of PHI Upon Termination. Upon termination or expiration of this BAA for any reason, Business Associate shall return to EC3Health or destroy any PHI received from EC3Health , or created, maintained, or received by Business Associate on behalf of EC3Health , that Business Associate still maintains in any form. Business Associate shall not retain any copies of such PHI. This requirement applies to PHI in the possession of Business Associate’s subcontractors or agents as well. However, if Business Associate determines that returning or destroying PHI is not feasible (for example, if the PHI must be retained for legal archival purposes, or if stored in backups that cannot be segregated), Business Associate shall notify EC3Health in writing of the conditions that make return or destruction infeasible. If EC3Health agrees, Business Associate shall extend the protections of this BAA to the retained PHI and limit further uses and disclosures to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains the PHI. Any PHI retained shall be maintained in accordance with this BAA’s confidentiality and security requirements, and any use or disclosure of the retained PHI shall continue to be limited to the same extent as prior to termination. Once the retention period or purpose expires, Business Associate must then proceed to delete or return the PHI.

6.4 Survival. The obligations of Business Associate under this BAA shall survive termination of the BAA and the Underlying Agreement with respect to any PHI that is not returned or destroyed. Additionally, the duty to report breaches, the indemnification obligations stated herein, and any provisions which by their nature should survive shall remain in effect.

7. General Provisions

7.1 Regulatory References. A reference in this Agreement to a section in the CFR or other law means that section as in effect or as amended, and for which compliance is required. The Parties intend that this Agreement shall at all times comply with the mandatory requirements of HIPAA, HITECH, and applicable state laws. Any ambiguity in this Agreement shall be interpreted to permit compliance with the most stringent applicable law.

7.2 Modification in Law. The Parties acknowledge that state and federal laws relating to data privacy and security are rapidly evolving. In the event any relevant provision of HIPAA, HITECH, CCPA, the SHIELD Act, or other privacy/security law is materially amended, enacted, or interpreted in a way that the terms of this BAA would not be compliant or would conflict with the new requirements, the Parties agree to negotiate in good faith to amend this BAA to ensure compliance. If the Parties are unable to agree on an appropriate amendment by the compliance date of the change in law, then either Party may terminate the Underlying Agreement and this BAA upon written notice, if permitted, or if a shorter period is required by law, the Parties will take interim steps to comply until an amendment is finalized.

7.3 Precedence; Incorporation. This BAA is attached to and made a part of the Underlying Agreement between the Parties. All terms and conditions of the Underlying Agreement remain in force except to the extent they contradict or are inconsistent with this BAA, in which case the terms of this BAA shall control with regard to the subject matter herein. This Agreement and the Underlying Agreement shall be interpreted as consistent wherever possible; however, if a specific conflict arises, the more protective term for PHI or the term required by law shall govern. Any references in the Underlying Agreement to compliance with health information privacy laws or to a business associate agreement are deemed to refer to this BAA.

7.4 No Third Party Beneficiaries. There are no third party beneficiaries to this Agreement. The Parties do not intend to create any rights for any third parties through this BAA. Those individuals' rights and remedies are governed by HIPAA and other applicable laws, not by this contract. Nothing in this Agreement shall be construed to grant any person or entity that is not a signatory to this Agreement any rights or remedies.

7.5 Indemnification. See Underlying Agreement.

7.6 Notices. Any notice required under this BAA to either Party shall be in writing and provided to the contact designated for notices in the Underlying Agreement. Notices regarding breaches or Security Incidents shall be sent to EC3Health's privacy or security official and to an email or address provided by EC3Health for urgent security notifications. Similarly, EC3Health shall send any notices to Business Associate's designated privacy officer or other contact as identified by Business Associate. Notices shall be deemed given as specified in the Underlying Agreement's notice provisions. The Parties shall ensure that contact information for notice remains up-to-date and shall promptly inform the other of any changes.

7.7 Governing Law. This BAA is governed by the same law that governs the Underlying Agreement, except to the extent preempted by federal law. (HIPAA preempts conflicting state law unless the state law is more stringent, in which case this Agreement effectively incorporates that state law standard by reference as discussed.) Any action or proceeding arising from or relating to this Agreement shall be brought in the forum specified in the Underlying Agreement, and the Parties hereby consent to such jurisdiction as applicable.

7.8 Counterparts and Electronic Signatures. This Agreement 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. Signatures transmitted electronically shall be binding as originals.

7.9 Entire Agreement. This BAA, together with the Underlying Agreement, constitutes the entire agreement between the Parties with respect to the specific subject matter of PHI privacy and security, and supersedes all prior discussions, negotiations, or understandings relating thereto. In the event of any inconsistency between the terms of this BAA and the Underlying Agreement or any other agreement between the Parties, the terms of this BAA shall prevail with regard to the use, disclosure, and protection of PHI. Any amendment to this BAA must be made in writing and signed by both Parties.
[END TERMS] [SIGNATURE PAGE FOLLOWS] [REMAINDER OF PAGE LEFT BLANK]

IN WITNESS WHEREOF, the Parties have caused this Business Associate Agreement to be executed by their duly authorized representatives as of the Effective Date written above.

EC3Health

By:_____

Name:_____

Date Signed:_____

DNA Regimen, LLC

By:_____

Name:_____

Date Signed:_____

[END AGREEMENT][REMAINDER OF PAGE LEFT BLANK]