STATE OF TEXAS §
§
COUNTY OF FORT BEND §

ADDENDUM TO VIRGIN PULSE'S AGREEMENT

(Utilizing Sourcewell Contract No. 051922-VRG)

This Addendum ("Addendum") is made and entered into by and between FORT BEND COUNTY, TEXAS ("County"), a political subdivision of the state of Texas, and Virgin Pulse, Inc. ("Virgin Pulse"), a corporation authorized to conduct business in the state of Texas. County and Virgin Pulse may be referred to individually as a "Party" or collectively as the "Parties."

WHEREAS, Virgin Pulse provides a social wellness platform known as Ignite, which helps organizations cultivate healthy cultures and workplaces (the "Services"); and

WHEREAS, County desires to purchase such Services from Virgin Pulse for the benefit of County pursuant to Sourcewell Contract No. 051922-VRG; and

WHEREAS, Virgin Pulse's Order Form for the above-referenced Services includes attached Appendices A – E (hereinafter, "Virgin Pulse's Agreement") which provides certain terms of service; and

WHEREAS, subject to the modifications provided in this Addendum, County has agreed to the terms of Virgin Pulse's Agreement; and

WHEREAS, the Addendum and the Virgin Pulse's Agreement are hereinafter collectively referred to as the "Agreement"; and

WHEREAS, this Agreement is not subject to competitive bidding requirements under Section 271.102 of the Texas Local Government Code which authorizes County's participation in a cooperative purchasing program.

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties do mutually agree as follows:

1. **Recitals.** The recitals set forth above are incorporated herein by reference and made a part of this Agreement.

2. **Scope of Services.** Pursuant to Sourcewell Contract No. 051922-VRG, and subject to the terms of this Addendum, Virgin Pulse shall provide the Services to County as described in Virgin Pulse's Agreement attached hereto as Exhibit "A" and incorporated by reference for all intents and purposes.

3. **Term.** The Agreement shall be effective on the date it is fully signed by all Parties (the "Effective Date") and will expire on the Initial Order End Date as set forth in the attached Exhibit "A" (the "Initial Term"), unless sooner terminated in accordance with the terms provided herein. There shall be no automatic extensions or renewals of the Agreement upon the expiration of the Initial Term. However, the Parties shall have the option to renew the Agreement under the same terms and conditions for two (2) additional one (1) year "Renewal Terms" provided that such renewal is in writing and signed by each of the Parties hereto.

4. **Fee Increases.** County and Virgin Pulse agree that any Renewal Terms shall be subject to a renegotiation of the Subscription Fees. Therefore, any reference to a renewal increase of the Subscription Fees in Section 5.4, Appendix B of Virgin Pulse's Agreement are hereby inapplicable to County and removed.

5. **Initial Order Start Date.** Notwithstanding any provision to the contrary herein, the Services shall be made available for use on the Initial Order Start Date as provided in the attached Exhibit "A."

6. **Compensation and Payment Terms.**

   (a) Virgin Pulse's fees for the Services provided under this Agreement shall be calculated at the rate(s) set forth in Virgin Pulse's Agreement attached hereto as Exhibit "A."

   (b) County will pay Virgin Pulse based on the following procedures in addition to those procedures set forth in Section 7 of this Addendum and Section 5.1 of Appendix B: Virgin Pulse shall submit to County an invoice showing the amounts due. Virgin Pulse may submit electronically via: apauditor@fortbendcountytx.gov. County shall review such invoices and approve and pay such approved invoice within thirty (30) calendar days as set forth in Section 5.1 of Appendix B.

7. **Limit of Appropriation.**

   (a) The Parties acknowledge and agree that the costs for the Services provided by Virgin Pulse to County under this Agreement is based on the number of units committed by County (the "Total Costs"). In the event the number of units is increased by County during any term year, Virgin Pulse shall conduct billing adjustments based on the actual number of units provided by County and shall invoice County as provided in Section 6 of this Addendum and Section 5.1 of Appendix B.

   (b) Notwithstanding the foregoing, County represents and warrants to Virgin Pulse that, as of the Effective Date of this Agreement, the Commissioners Court of Fort

Bend County, Texas has identified appropriated, and set aside sufficient monies to fund the Total Costs of the Services in the amount of Seventy Two Thousand Two Hundred Ninety Nine and 00/100 Dollars ($72,299.00). In no event shall County's liability for and obligation to pay the Total Costs of the Services exceed the amount of $72,299.00 unless such excess cost is itemized and provided to County in advance and approved by County as evidenced by the issuance of a County approved change order.

(c) Subject to Section 7(b) of this Addendum, Virgin Pulse understands and agrees that the total maximum compensation that Virgin Pulse may become entitled to and the total maximum sum that County may become liable to pay to Virgin Pulse under this Agreement shall not under any conditions, circumstances, or interpretations thereof exceed the amount of $72,299.00 without a County approved change order.

8. **Payment of Fees and Penalties by County.**

(a) Virgin Pulse understands and agrees that County is a political subdivision of the state of Texas and subject to the Texas Constitution and the laws of the state of Texas which expressly prohibit County from lending its credit or gratuitous applications of public funds. The Texas Constitution and laws of the state of Texas also prohibit County from payment of any penalties. As such, the second sentence of Section 5.1 of Appendix B in Virgin Pulse's Agreement is hereby inapplicable to County and removed, to the extent that it is prohibited by applicable law.

(b) Notwithstanding the foregoing, should the County, in good faith, object to or dispute any portion of the County's payment to Virgin Pulse, the County shall notify Virgin Pulse of the specific objection or dispute in writing within 10 calendar days of its receipt of Virgin Pulse's Invoice, and may withhold payment of the disputed amount pending resolution of the dispute. The Parties shall attempt, in good faith, to resolve such dispute within sixty (60) days of Virgin Pulse's receipt of County's written notice. In the event the Parties are unable to resolve such dispute, then: (1) either Party may pursue any remedy available at law or in equity to enforce its rights hereunder; and (2) Virgin Pulse reserves the right to suspend access to the Solution until the dispute is resolved. Any undisputed portions of the invoice shall be paid by County in accordance with the terms of this Agreement. Any withholding of payment by County under this subsection shall not be deemed to be a breach or default of this Agreement. For the avoidance of doubt, if Virgin Pulse appropriately assesses fees on an invoice based on the number of Eligibles included on a County Eligibility File, then the Parties agree that insufficient funding from the County shall not be deemed a basis for disputing a payment. If Virgin Pulse does not receive payment of any undisputed sum due to it within thirty (30) days of the invoice, Virgin Pulse reserves the right to suspend access to the Solution, including but not limited to the Members' ability to accrue or redeem any rewards, until such time as the default has been cured to Virgin

Pulse's satisfaction. Notwithstanding anything to the contrary herein, all invoiced amounts for rewards are due and payable within thirty (30) days of the date of Provider's invoice.

9. **Taxes.** County is a political subdivision of the state of Texas and as such, is exempt from sales and use taxes. County shall furnish evidence of its tax-exempt status to Virgin Pulse.

10. **Indemnity. TO THE EXTENT THAT COUNTY IS PROHIBITED BY APPLICABLE LAW FROM DEFENDING, INDEMNIFYING, HOLDING, OR SAVING HARMLESS VIRGIN PULSE OR ANY OTHER PARTY, FOR ANY REASON WHATSOEVER, THEN ANY PROVISION OF THE AGREEMENT REQUIRING THE SAME SHALL BE INAPPLICABLE TO COUNTY AND REMOVED.**

11. **Applicable Law; Arbitration; Attorney Fees.** The laws of the state of Texas govern all disputes arising out of or relating to this Agreement. The Parties hereto acknowledge that venue is proper in Fort Bend County, Texas for all legal actions or proceedings arising out of or relating to this Agreement and waive the right to sue or be sued elsewhere. County does not agree to submit disputes arising out of or related to the Agreement to binding arbitration. Therefore, any references to binding arbitration or the waiver of a right to litigate a dispute in Virgin Pulse's Agreement are hereby inapplicable to County and removed. Additionally, County does not agree to pay any and/or all attorney fees incurred by Virgin Pulse in any way associated with this Agreement.

12. **No Waiver of Jury Trial.** The County does not agree that all disputes (including any claims or counterclaims) arising from or related to this Agreement shall be resolved without a jury. Therefore, any references in Virgin Pulse's Agreement to County's waiver of jury trial are hereby inapplicable to County and removed.

13. **Public Information Act.** Virgin Pulse expressly acknowledges and agrees that County is a public entity and as such, is subject to the provisions of the Texas Public Information Act under Chapter 552 of the Texas Government Code. In no event shall County be liable to Virgin Pulse for release of information pursuant to Chapter 552 of the Texas Government Code or any other provision of law. Except to the extent required by law or as directed by the Texas Attorney General, County agrees to maintain the confidentiality of information provided by Virgin Pulse expressly marked as proprietary or confidential. County shall not be liable to Virgin Pulse for any disclosure of any proprietary or confidential information if such information is disclosed under Texas law or at the direction of the Texas Attorney General. To the extent required by law or as directed by the Texas Attorney General, the terms of this Agreement shall not be considered proprietary or confidential information.

14. **Compliance with Laws.** Virgin Pulse shall comply with all federal, state, and local laws, statutes, ordinances, rules, regulations, and the orders and decrees of any courts or administrative bodies or tribunals in any matter affecting the performance of this Agreement, including, without limitation, Worker's Compensation laws, minimum and maximum salary and wage statutes and regulations, licensing laws and regulations. Virgin Pulse in providing all services hereunder, further agrees to abide by the provisions of any applicable Federal or State Data Privacy Act.

15. **Independent Contractor.** In the performance of work or services hereunder, Virgin Pulse shall be deemed an independent Contractor, and any of its agents, employees, officers, or volunteers performing work required hereunder shall be deemed solely as employees of Virgin Pulse or, where permitted, of its subcontractors. Virgin Pulse and its agents, employees, officers, or volunteers shall not, by performing work pursuant to this Agreement, be deemed to be employees, agents, or servants of County and shall not be entitled to any of the privileges or benefits of County employment.

16. **Use of Customer Name.** Except as set forth in Appendix B of Exhibit "A", Virgin Pulse may use County's name without County's prior written consent only in Virgin Pulse's customer lists. Any other use of County's name by Virgin Pulse must have the prior written consent of County.

17. **County Data**. Nothing in this Agreement shall be construed to waive the requirements of Section 205.009 of the Texas Local Government Code. Additionally, Virgin Pulse agrees to notify County in writing prior to the deletion of any County data.

18. **Notice.** Any notice required to be given under the provisions of this Agreement shall be in writing and shall be duly served when it shall have been delivered in person or deposited, enclosed in a wrapper with the proper postage prepaid thereon, and duly registered or certified, return receipt requested, in a United States Post Office, addressed to a Party at the following addresses. If mailed, any notice or communication shall be deemed to be received three (3) business days after the date of deposit in the United States Mail. Unless otherwise provided in this Agreement, all notices shall be delivered to the following addresses:

Virgin Pulse	Virgin Pulse, Inc. Attn: Legal Department 75 Fountain St., Ste 310 Providence, Rhode Island 02902
County:	Fort Bend County Risk Management Attn: Wyatt Scott 301 Jackson St. Richmond, Texas 77469

With a copy to: Office of the Fort Bend County Judge
401 Jackson St.
Richmond, Texas 77469

Any Party may designate a different address by giving the other Party ten (10) calendar days' written notice.

19. **Personnel.** Virgin Pulse represents that it presently has, or is able to obtain adequate qualified personnel in its employment for the timely performance of the Services required under this Agreement and that Virgin Pulse shall furnish and maintain, at its own expense, adequate and sufficient personnel, in the opinion of County, to perform the Services when and as required and without delays.

All employees of Virgin Pulse shall have such knowledge and experience as will enable them to perform the duties assigned to them. If any employee of Virgin Pulse or agent of Virgin Pulse who, in County's opinion, is incompetent or by his conduct become detrimental to providing Services pursuant to this Agreement, then County shall notify Virgin Pulse in writing of such incompetency or conduct. The Parties shall thereafter, in good faith, attempt to address and resolve the same within such time as agreed to by the Parties. Such resolution may include but is not limited to the removal of such employee(s) or agent(s) from association with the Services provided under this Agreement.

20. **Remote Access**. As applicable, if Virgin Pulse requires remote access to County Systems for support, installation, integrations, configurations, and/or maintenance of Virgin Pulse's product and/or services, except as otherwise agreed by the parties and approved by County, the below requirements must be met before Virgin Pulse is granted remote access to County Systems:

(a) Virgin Pulse will adhere to the restricted and monitored channels that are provided by the County, or other technologies approved in advanced in writing by the County's Director of Information Technology and Chief Information Officer.

(b) Virgin Pulse will neither implement nor deploy a remote access solution which bypasses and/or is designed to bypass County provided or approved controls. Virgin Pulse will not access County Systems via unauthorized methods.

(c) Remote access is restricted only to County Systems necessary for Virgin Pulse to conduct their services and/or provide applicable product to County pursuant to this Agreement.

(d) Virgin Pulse will allow only its Workforce approved in advance by County to access County Systems. Virgin Pulse will promptly notify County whenever an individual member of Virgin Pulse's Workforce who has access to County Systems leaves its

employ or no longer requires access to County Systems. Virgin Pulse will keep a log of access when its Workforce remotely accesses County Systems. Virgin Pulse will supply County with evidence of access logs concerning remote access to County Systems upon written request from County. Such access logs will be provided to County, within three business days from the date of County's request. These requests may be used to confirm compliance with these terms and/or to investigate a security incident.

(e) If any member(s) of Virgin Pulse's Workforce is provided with remote access to County Systems, then Virgin Pulse's Workforce will not remotely log-in to County Systems from a public internet access device (e.g., airport computer terminal, or Internet café). This is due to the possibility of sensitive information being monitored by video or computer surveillance in public areas.

(f) Failure of Virgin Pulse to comply with this Section may result in Virgin Pulse and/or Virgin Pulse's Workforce losing remote access to County Systems. County reserves the right at any time to disable remote access to protect County Systems.

(g) For purposes of this Section, "Workforce" means employees, agents, subVirgin Pulses (where permitted), and/or other persons whose conduct, in the performance of work for Virgin Pulse, is under the direct control of Virgin Pulse, whether or not they are paid by Virgin Pulse and who have direct or incidental access to County Systems.

(h) For purposes of this Section, "Systems" means any: (i.) computer programs, including, but not limited to, software, firmware, application programs, operating systems, files and utilities; (ii.) supporting documentation for such computer programs, including, without limitation, input and output formats, program listings, narrative descriptions and operating instructions; (iii.) data and/or media; (iv.) equipment, hardware, servers, and/or devices; and/or (v.) network(s).

21. **Entire Agreement and Modification.** This Agreement constitutes the entire Agreement between the Parties and supersedes all previous agreements, written or oral, pertaining to the subject matter of this Agreement. Any amendment to this Agreement must be in writing and signed by each Party to come into full force and effect.

22. **Understanding Fair Construction.** By execution of this Agreement, the Parties acknowledge that they have read and understood each provision, term, and obligation contained herein. This Agreement, although drawn by one party, shall be construed fairly and reasonably and not more strictly against the drafting Party than the non-drafting Party.

23. **Severability.** In case any one or more of the provisions contained in this Agreement shall for any reason be held to be invalid, illegal or unenforceable in any respect, such invalidity,

illegality or unenforceability shall not affect any other provision hereof and this Agreement shall be construed as if such invalid, illegal or unenforceable provision had never been contained herein.

24. **No Waiver of Immunity.** Neither the execution of this Agreement nor any other conduct of either party relating to this Agreement shall be considered a waiver or surrender by County of its governmental powers or immunity under the Texas Constitution or the laws of the state of Texas.

25. **Conflict**. In the event of a conflict between Virgin Pulse's Agreement attached hereto and the terms of this Addendum, this Addendum shall prevail.

26. **Certain State Law Requirements for Contracts** The contents of this Section are required by Texas law and are included by County regardless of content For purposes of Sections 2252.152, 2271.002, and 2274.002, Texas Government Code, as amended, Virgin Pulse hereby verifies that Virgin Pulse and any parent company, wholly owned subsidiary, majority-owned subsidiary, and affiliate:

(a) Unless affirmatively declared by the United States government to be excluded from its federal sanctions regime relating to Sudan or Iran or any federal sanctions regime relating to a foreign terrorist organization, is not identified on a list prepared and maintained by the Texas Comptroller of Public Accounts under Section 806.051, 807.051, or 2252.153 of the Texas Government Code.

(b) If employing ten (10) or more full-time employees and this Agreement has a value of $100,000.00 or more, Virgin Pulse does not boycott Israel and is authorized to agree in such contracts not to boycott Israel during the term of such contracts. "Boycott Israel" has the meaning provided in § 808.001 of the Texas Government Code.

(c) If employing ten (10) or more full-time employees and this Agreement has a value of $100,000.00 or more, Virgin Pulse does not boycott energy companies and is authorized to agree in such contracts not to boycott energy companies during the term of such contracts. "Boycott energy company" has the meaning provided in § 809.001 of the Texas Government Code.

(d) If employing ten (10) or more full-time employees and this Agreement has a value of $100,000.00 or more, Virgin Pulse does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association and is authorized to agree in such contracts not to discriminate against a firearm entity or firearm trade association during the term of such contracts. "Discriminate against a firearm entity or firearm trade association" has the meaning provided in § 2274.001(3) of the Texas Government Code. "Firearm

entity" and "firearm trade association" have the meanings provided in § 2274.001(6) and (7) of the Texas Government Code.

27. **Human Trafficking.** BY ACCEPTANCE OF THIS AGREEMENT, VIRGIN PULSE ACKNOWLEDGES THAT FORT BEND COUNTY IS OPPOSED TO HUMAN TRAFFICKING AND THAT NO COUNTY FUNDS WILL BE USED IN SUPPORT OF SERVICES OR ACTIVITIES THAT VIOLATE HUMAN TRAFFICKING LAWS.

28. **Captions.** The section captions used in this Agreement are for convenience of reference only and do not affect the interpretation or construction of the Agreement.

29. **Electronic and Digital Signatures.** The Parties to this Agreement agree that any electronic and/or digital signatures of the Parties included in this Agreement are intended to authenticate this writing and shall have the same force and effect as the use of manual signatures.

30. **Certification.** By his or her signature below, each signatory individual certifies that he or she is the properly authorized person or officer of the applicable Party hereto and has the requisite authority necessary to execute this Agreement on behalf of such Party, and each Party hereby certifies to the other that it has obtained the appropriate approvals or authorizations from its governing body as required by law.

{Execution Page Follows}

IN WITNESS WHEREOF, and intending to be legally bound, County and Virgin Pulse hereto have executed this Agreement to be effective on the date of full execution by all Parties.

FORT BEND COUNTY, TEXAS	**VIRGIN PULSE, INC.**
	DocuSigned by: AB4E7Q8AB6CA47B...
KP George, County Judge	Authorized Agent – Signature
	Rik Thorbecke
Date	Authorized Agent – Printed Name
	Chief Financial Officer
ATTEST:	Title
	7/27/2023
	Date
Laura Richard, County Clerk	DocuSigned by: Gina Simonelli Baxter 7093A0F155EE445...
	Approved by

AUDITOR'S CERTIFICATE

I hereby certify that funds in the amount of **$_____** are available to pay the obligation of Fort Bend County, Texas within the foregoing Agreement.

Robert Ed Sturdivant, County Auditor

i:\agreements\2023 agreements\risk management\virgin pulse (23-risk-100495)\addendum - virgin pulse.docx - JLF

EXHIBIT A

(Includes all Appendices attached hereto)

Order Form: Virgin Pulse – Sourcewell Contract #051922-VRG

Order Form Prepared for:	**Fort Bend County, TX**	Bill To Address:	County to provide
Prepared By:	**Rachel Grossman**	Contact Name:	County to provide
Order Form Expiration Date: 3/31/2023		Contact Email:	County to provide
		Contact Phone:	County to provide

This Order Form ("**Order Form**") is entered into as of the date last signed by both Parties below ("**Effective Date**") and incorporates by reference the following appendices (collectively, the "**Agreement**):

Appendix A – Solution Descriptions
Appendix B – Terms & Conditions
Appendix C – Data Security Standards
Appendix D – Business Associate Agreement
Appendix E – Optional Services Attachment

This Agreement shall be legally binding as of the Effective Date and, unless terminated in accordance with the Terms & Conditions, continue until the "**Initial Order End Date**" set forth in the table below (the "**Agreement Term**").

Selected Services & Fees

Services	Initial Order Start Date	Initial Order End Date	Initial Order Term (years)	Billing Unit	Price Per Unit	Minimum Units Committed	Estimated Units	Total Price Per Year
Platform: Ignite for Employees	01/02/2024	01/01/2025	1 years	Flat fee of $69,400 for up to 2,500 Eligibles	$27.76 PEPY for each Eligible above 2,500	2,500	2,500	$69,400
Platform: Ignite for spouses/domestic partners	01/01/2024	01/01/2025	1 years	PEPY Fee Waived	$0	$0	NA	$0
Implementation	-	-	-	One-time Fee waived	$0	-	-	$0
Max Buzz Activity Tracker	-	-	-	Per Unit	$28.99	100	100	$2,899
Custom Communications Service Credit	-	-	-	Annual Credit	($7,500)	-	-	$0
Custom Communications Services	-	-	-	Hourly	$150	-	-	$0
Custom Reporting Service Credit	-	-	-	Annual Credit	($4,000)	-	-	$0
Custom Reporting Services	-	-	-	Hourly	$200	-	-	$0
						Year One Fees:		**$72,299**

Payment Terms and Conditions:

1. For those Services listed above with an eligibility-based Billing Unit, the Selected Services Fees will be invoiced annually in advance on the Initial Order Start Date and on the anniversary of thereafter for the duration of the Term, based on the greater of the (a) Minimum Number of Units Committed as set forth in the Table above; or (b) the actual number of Units on record in Provider's system at the time of invoice. Any increase in the number of Units above the invoiced number of Units in a given year will result in a pro-rated price for such additional Units for that year and invoiced quarterly.
2. Billing Definitions: PEPY=Per Eligible Per Year.
3. 10 SSO's (inbound or outbound) included at no additional cost.
4. The Communications Service Credit is annual and expires at the end of each program year. Unused credit cannot be carried over each year; it cannot be applied to non-communication related services (e.g., reporting). It cannot be applied to hard costs like printing of materials or postage for shipping, or language translation services.
5. Custom Reporting Service Credit is annual and expires at the end of each program year. Unused credit cannot be

carried over each year.

6. Optional Services are as set forth in the Optional Services Attachment attached hereto as Appendix E. Pricing and availability as set forth in the Optional Services Attachment is subject to change and will be confirmed within an agreed upon Amendment or Statement of Work.
7. Rewards will be invoiced bi-monthly in arrears based on the total value of rewards earned by each Member during the applicable period.

The Parties have caused their duly authorized representatives to execute this Agreement as of the dates set forth below.

CLIENT:	_____	**VIRGIN PULSE, INC.**	
By (Signature):	_____	**By (Signature):**	_____
Name (Printed):	_____	**Name (Printed):**	_____
Title:	_____	**Title:**	_____
Date:	_____	**Date:**	_____

APPENDIX A: SOLUTION DESCRIPTIONS

Product descriptions may be updated from time to time to reflect feature changes.

PRODUCT CAPABILITIES

Platform Design & Configurations	**Branding, Theming & Content Organization** Configure platform elements to reflect your culture and brand. Align content and wellbeing pillars to your organizational focus areas. **Personalization Engine** Targeted programming and content delivered in an automated fashion to members based on their interests, health risks, & demographics to ensure a personalized experience. **Incentive Management Framework** Configure incentive structures to your requirements. Reward options can be outcomes-based, task-based, and/or points-based designs. As members engage in healthy behaviors and participate in differing activities, they can earn rewards, i.e., cash, healthcare contributions, local incentives, or store credits. Incentives can be segmented by employee group, i.e., employee vs spouse, US vs. International. Incentive management can be facilitated through the VP platform and/or VP can provide reporting to you to administer the incentive. **Integration Framework** Integrate specific benefits and programming to your population. Configure available programs determined by client. Integrate and promote benefits, tools, events, and information to drive awareness, usage and impact both on-platform via web & mobile and off-platform. Integrate client-specific programming as well as Virgin Pulse partnerships with the potential for data transfer and rewarding. **Language Options** The platform and mobile app are available in the following languages: US English, UK English, Chinese (Simplified), Chinese (Traditional), French (European), French (Canadian), German, Italian, Japanese, Korean, Malay, Polish, Portuguese (Brazilian), Russian, Spanish (Latin American), Spanish (European), Swedish, Vietnamese, Dutch, Thai, and Hindi.

Habit Building & Behavior Change Tools	**Healthy Habit Trackers** Members self-track health and wellbeing behaviors in key areas: activity, nutrition, learning, sleep, community, relationships, stress, productivity, financial wellbeing, safety, sustainability, diversity, inclusion, and effectiveness, with the intent of prompting members to make small but daily changes in their lifestyle. **Daily Health & Wellbeing Tips** Members receive personalized daily tip cards based on their selected interests. The cards take a micro-learning and small steps approach to cue healthy actions. The tip cards encompass key areas: activity, nutrition, learning, sleep, community, relationships, stress, productivity, financial wellbeing, safety, sustainability, diversity, inclusion, and effectiveness. **Digital Coaching** Virgin Pulse Journeys® are daily, self-guided courses that breaks a key behavior or a larger goal into smaller achievable steps, helping people improve their health literacy and form new habits as they go. They cover a variety of lifestyle and health related topics including topics such as, nutrition, stress, finance, and tobacco. **Sleep & Nutrition Modules** Personalized plans that provide practical guidance and a framework to adopt healthy habits with tracking tools, resources, and tips, & reminders. **Challenges** Corporate and Peer competitions that drive step increases and/or healthy habit development. Also includes promotions and configuration options. Supported challenge types include destination, staged, basic, charity, spotlight, cross-sponsor, family, and healthy habits. **Social Connections** Members can connect with colleagues, leverage a leaderboard to show activity among friends and join groups based on interests. Additionally, members can invite up to 10 Friends & Family to participate in a limited experience. **Shoutouts** An employee and peer recognition tool to facilitate a culture of recognition and appreciation and drive engagement with company values.
Assessment & Measurement	**Health Assessment – Health Check** Flagship assessment that leverages NCQA-certified content to offer members a fresh look at their lifestyle choices and personal health. **Surveys** Client-built custom surveys that can segmented and deployed through VP platform. Surveys include reporting to help clients act on the insights provided by their population.
Condition Management	**My Care Checklist** My Care Checklist provides personalized reminders based on data and HEDIS measures to help members stay on top of condition-specific and preventive care actions throughout the year.

ADMINISTRATIVE RESOURCES

Admin Portal	**Admin Portal** Program administrators can use web-based management tools to manage and segment components of their Virgin Pulse program including calendar events to promote events broadly or to specific locations. There is also the ability to configure wellbeing pillars and topics. Administrators can create daily cards and healthy habits for their employees. Lastly, this tool may be used to deploy unlimited Destination, Basic and Healthy Habit challenges. Choose from the Virgin Pulse Challenge Theme Library or create your own custom theme (client supplies custom content and images), and configure challenge settings (start/end dates, etc.)
Program Reporting & Analytics	**On-Demand Reporting** Program administers will have 24/7 access to on-demand, self-serve analytics dashboard to configure and access a range of reports, track member engagement, measure outcomes, and tailor content and programming in real-time. Refreshed daily, metrics may be filtered by organizational hierarchy, rewards segmentation, and many other attributes, providing all the information necessary to manage diverse populations. Reports can be explored as Excel, CSV, and PowerPoint files for easy viewing and additional analysis. **On-Demand Reporting Dashboards Include:** Participation: Easy to access and highly visual key metric overview gives you the pulse of your program and your workforce with real-time participation, engagement and location-specific reporting that help you put your data to work for your organization. At-a-Glance Executive View Enrollment Engagement Risk: Virgin Pulse Analytics eliminates data silos by bringing all your biometric solutions together on one platform for a complete view into your population's risk profile. HRA Biometrics Utilization: Deep engagement and participation metrics deliver valuable insight into the wellbeing areas of highest interest to your employees. Levels and Incentives Corporate Challenges External Programs Topics **Self-Serve Data Extracts** Monthly member-level reporting automatically uploaded to Program administrators account to support internal reporting needs. Eligibility Report Member Activation Billable Cash Earned Report Non-Billable Cash Device Subsidy Orders Month End (if applicable) Coaching Month End (if applicable) **Standard Data Extracts** Monthly member-level reporting available upon request. Delivered for current reported month and in standard file format only. Account Manager will work with Program Administrator to determine applicable reports and cadence. Challenge Activity Healthy Habit Tracking Levels & Points Activity Complete Aggregated Rewards Trigger Device Subsidy and Shipping Reward and Incentive Drawing File

	Billable Cash Tobacco Non-standard data feeds that require customization may incur a professional services rate of $200 per hour. **Claims Reporting** Medical and pharmaceutical PDF report aggregating claims risk, conditions, gaps and gaps in closure for participants and non-participants within cohort and total population. **Client Reviews** Strategic review of all programming delivered with insightful recommendations. The Virgin Pulse Client Success team follows a consultative and collaborative support methodology. The Client Review is a critical part of the process and a key time for an in-depth analysis of data sets and KPIs relevant to your organization. Your Client Success Manager (CSM) will present an exhaustive, detailed analysis across all your program data, evaluate and uncover program highlights, trends, insights and opportunities, review strategic recommendations, detailed plans and Virgin Pulse product roadmap. **Custom Reporting Services Credit** The Custom Reporting Service Credit is annual and expires at the end of each program year. Clients may apply the credit towards the creation of any custom report type not available as standard. Any custom reporting outside of the credit will be billed at $200/HR.

COMMUNICATIONS

Communications	**Standard Member Communications** Includes launch campaign options with emails, posters, digital displays, and leadership kit to support enrollment. Additionally, on-going auto-generated comms are delivered to individuals based on their interactions with the platform via email and/or mobile app. **Custom Communications Services Credit** The Communications Service Credit is annual and expires at the end of each program year. Applicable examples of custom deliverables include: Modification of Catalog Email Multi-channel Custom Comms Campaign New Custom Email Site Pop-Ups In-app messages / Mobile Push Notifications Print-Ready Posters / Digital Displays Print-Ready Post Card Content for Custom Challenges, Healthy Habits, and Daily Cards Custom Video Work (travel expenses billed separately) Third Party Expenses, such as travel, printing and translation, will be billed separately

ACCOUNT MANAGEMENT SERVICES

Account Management Services	An account manager will be responsible for proactive program management and client outreach to optimize program performance. Services will include: Recurring program strategy calls with account manager Annual program review with focus on mutually agreed upon KPI's Comprehensive annual planning process Annual review of Virgin Pulse Product Roadmap Access to Client Service Portal, a self-service ticketing tool where clients can request feature configuration changes, custom content and support on member issues Ability to create one (1) custom Basic or Destination challenge per year for clients, as requested. Client supplies custom content and images. Ability to configure one (1) Basic or Destination challenges from the Challenge Theme Library per year for clients, as requested. For Destination challenges, client has option to supply custom destination content and images for up two (2) of the challenge locations. Client newsletter including new feature announcements and engagement promotion updates Invitation to the annual Virgin Pulse Thrive conference

MEMBER SERVICES SUPPORT

Online Support	Members may access a knowledgebase of helpful program information and problem resolutions via the Support section of the program site or they may submit questions via the Support form.
Member Services	Provides member-level support after launch via phone (888-671-9395) and email (support@virginpulse.com) from 8am-9pm EST, Monday-Friday; and chat 2am-9pm EST, Monday-Friday.

IMPLEMENTATION SERVICES

Implementation Services	All clients have a designated Implementation Project Manager who is responsible for facilitating and coordinating execution of program launch. Services include: Designated Implementation Project Manager Scheduled implementation meetings with client and any 3rd party vendors Platform and incentive design consulting & forecasting Facilitation of IT requirements review and validation Setup, mapping, and testing of initial eligibility file and ongoing eligibility file process Configuration and QA of Virgin Pulse platform and client's program design Setup of applicable reward redemption options and ecommerce store Coordination, setup, and testing of file integrations with client's 3rd party vendors Coordination of communications strategy; delivery of Launch Comms & Champions pre-launch [if applicable] Configuration of initial corporate challenge Coordination of device fulfillment & logistics if applicable

OPTIONAL VIRGIN PULSE HARDWARE – ACTIVITY TRACKERS & HEALTH STATIONS

Virgin Pulse Hardware Tracking Devices	**Max Buzz** An activity and sleep tracking device with vibrating alerts for alarms and phone calls/text messages.

APPENDIX B: VIRGIN PULSE INC. TERMS & CONDITIONS

1. SCOPE, TERM, &TERMINATION

1.1 **Scope.** These Solution and Services Terms and Conditions ("**Terms**") are incorporated by reference into each Virgin Pulse Order Form ("**Order Form**") entered into between the entity listed on the Order Form ("**Client**") and Virgin Pulse, Inc., or any of its affiliates (each referred to as a "**Provider**") and governs the provision by Provider of its software-as-a-service products or mobile software applications ("**Products**"), current published guides for the Products ("**Documentation**"), its databases of individual demographic and behavioral data ("**Provider Data**"), deployment, support, integration, configuration, coaching, screening, guides, campaign, engagement or other related services ("**Services**"), and literary, graphic, video, audio, or photographic content resulting from the Services or displayed or distributed via the Products ("**Provider Content**"), (collectively, a "**Solution**"). In the event of any conflict between these Terms and an Order Form, these Terms shall govern, unless the Order Form expressly says otherwise. These Terms, the Order Form and all Appendices are collectively referred to as the "**Agreement**".

1.2 **Term.** The term of these Terms will commence on the Effective Date and shall continue thereafter until the sooner of expiration of all Order Forms or the termination of all Order Forms in accordance with this Section 1 ("**Term**").

1.3 **Termination for Breach.** Either Party may terminate this Agreement if: (i) the other Party makes an assignment for the benefit of creditors, ceases to do business, terminates its business operations, or becomes insolvent, or proceedings are instituted by or against it that are not terminated within sixty (60) days, (ii) the other Party materially breaches this Agreement and does not cure such failure within thirty (30) days' of receipt of notice from the non-breaching Party; or (iii) a change in Law occurs during the Term that materially and adversely impairs Provider's ability to provide the Solution and/or Services in compliance with Applicable Laws (as defined below) and the Parties acting in good faith are unable to reach agreement on an amendment to account for such change in Applicable Laws within a reasonable period of time, but no later than the first date on which the change in law becomes effective; *provided*, that Provider may immediately terminate this Agreement without prior notice or the opportunity to cure if the Client's material breach results in a violation any laws, regulations and orders of the United States relating to export controls and trade sanctions ("**US Export Controls and Trade Sanctions**").

1.4 **Effect of Termination**. Upon termination of this Agreement, all rights and licenses granted hereunder shall immediately cease; *provided, however*, that in the event there is any Order Form still in effect as of the effective date of termination, this Agreement shall remain in full force and effect solely with respect to such Order Forms until such Order Forms expire or are terminated in accordance with the terms of each Order Forms Within thirty (30) days of the termination date of this Agreement, Provider shall delete any Client Data in its possession or control and certify such deletion in writing to Client. Termination of this Agreement will not relieve either Party from any obligation or liability that has accrued prior to the effective date of termination, including Client's obligation to pay Provider for the Solution up to the date of termination. Upon Client's request, Provider, in its sole discretion, shall provide up to one-hundred eighty (180) days of assistance to Client for transition of the Solution at the prices agreed upon in the Order Form and any other services on a time and materials basis in accordance with a mutually-agreed upon rate card.

2. ACCESS AND LICENSE GRANTS.

2.1. **Access Grant**.

a. **By Provider.** During the Term, Provider grants to Client a non-exclusive, non-transferrable right to: (i) access and use the Solutions set forth in the applicable Order Form(s); and (ii) grant access to the Solutions to the number of persons provided to Provider by Client on an Eligibility File (subject to any quantity restrictions specified in the Order Form) (each "**Eligible**") for which Client has paid the applicable fees solely in accordance with the terms and conditions of this Agreement; (iii) and authorize such Eligibles to use the Solutions (each enrolled Eligible referred to as a "**Member**").

b. **By Client**. During the Term, Client grants to Provider a non-exclusive right to: (i) store, use, and process any data provided by Client (including Eligibility Files) ("**Client Data**") and/or any information provided by or on behalf of Members ("**Member Data**") to provide the Solutions specified in an Order Form; (ii) de-identify and aggregate Client Data and Member Data with data from other sources and/or Provider Data to improve its Products ("**Combined Data**"); and (iii) create and distribute derivative works that are based on Combined Data and/or Client Data that has been rendered unidentifiable but not aggregated ("**De-Identified Data**"). **Eligibility File** shall mean a file provided by Client to Provider in accordance with the applicable requirements outlined by Provider, containing at least the following information: the number of Eligibles and the Eligibles' last name, first name, date of birth, unique employee identifying number, if applicable, and any other information necessary to enable Provider to fulfill its obligations under the Agreement.

2.2 **License Grants.**

a. **By Provider.** During the Term, Provider hereby grants to Client a limited, non-exclusive, revocable, non-transferable, royalty-free (subject to payment of all applicable Fees) license, to download, reproduce, use, perform, and display (and to sublicense the foregoing rights to its Members): (i) the Products; (ii) any logos, trademarks, service marks, or content contained therein ("**Provider Brand**"); and/or (iii) any Provider Content made available or distributed by Provider in connection the applicable Solution.

b. **By Client.** During the Term, Client hereby grants to Provider a limited, non-exclusive, revocable, non-transferable, royalty-free license, without right to sub-license, to reproduce, translate, encode, publish, use, and display any logos, trademarks, service marks, or content provided by Client ("**Client Brand**") on any Client-branded interfaces or materials included in a Solution; and (ii) display the Client Brand in marketing materials solely for the purposes of identifying Client as a Client of Provider.

2.3 **Restrictions**. Client will not (a) copy or duplicate any Solution except as permitted herein; (b) modify, translate, decompile, disassemble, reverse engineer or otherwise reverse engineer any Solution or any portion thereof or create any derivative product from any of the foregoing, except with the prior written consent of Provider; or (c) assign, sublicense, sell, resell, lease, rent or otherwise transfer or convey, or pledge as security or otherwise encumber, Client's rights in any Solution.

3. OWNERSHIP.

3.1 **By Client.** Client owns all right, title and interest in and to the Client Brand, Client Data, Eligibility Files, and Client Confidential Information (as defined below) (collectively, the "**Client Materials**") and except for any rights granted herein, Provider acknowledges that it neither owns nor acquires any additional rights in and to the Client Materials. "**IP Rights**" means all patent, copyright, trademarks, trade secrets, know-how, techniques, concepts, ideas, methods, algorithms, models, formulas, and database rights, including any applications, continuations and goodwill.

3.2 **By Provider.** As between Client and Provider, Provider owns all right, title and interest in and to the Solutions and Provider Brand ("**Provider Materials**") and all IP rights therein, including any data related to, or derived from, the use and performance of any Solution or part of a Solution. Client acknowledges that: (a) Solutions are provided on a multi-tenant, access only-basis and (b) Client does not acquire any rights of ownership or exclusive use in any Provider Materials or in any derivative work thereof or work product produced as a result of using a Solution.

3.3 **By Member.** Provider manages Member Data for the benefit of such Members in accordance with this Agreement, applicable Law and Provider's Terms of Use, privacy policy, and any end-user agreements acknowledged by the applicable Member ("**Member Agreement**"). Nothing under this Agreement or any other agreement entered into between the Parties shall prevent or restrict Provider's ability to seek an Eligible's acceptance of Member Agreement prior to granting access to a Solution, which permits Provider to use Member Data for any lawful purpose, including as necessary for the operations, administration, and development of Provider's product or services and providing the Solutions to the applicable Member.

4. OBLIGATIONS.

4.1 **Provider Services.** During the Term, Provider shall (a) provide Client with monthly reports specifying quantity and activity participation of Members (to the extent permitted by applicable law and the Member Agreement); (b) fulfill incentives under Client's wellness program in accordance with Client's policies and upon Client's determination that a Member has not earned or is not entitled to incentive under a wellness program, provide a claims denial notice in the form and manner directed by Client, *provided, that* Client shall administer any appeal process; (c) adjust, remove, or recoup rewards accumulated in error or in a manner that violates the Membership Agreement or result from fraud; (d) upon Client's request, provide portable monitoring devices (each a "***Portable Device***") to Members for the additional fees for such Portable Devices which fees may be modified from time to time in Provider's sole discretion (subject to the Member Agreement and any restrictions imposed by US Export Controls or Trade Sanctions, ("**Sanctions**"); (e) perform any additional services mutually agreed upon by the parties in a Statement of Work ("**SOW**") or amendment to this Agreement; and (f) with respect to any Provider employee that performs Services under this Agreement, conduct standard background checks covering criminal history, including state, county and federal felonies and misdemeanor convictions, prior employment and education verification, I-9 completion, OIG and GSA sanctions checks.

4.2 **Client Obligations.** During the Term, Client shall provide: (a) provide all Client Materials (including Eligibility Files) necessary for Provider's implementation and performance of its obligations under this Agreement; (b) update Eligibility Files each month, including any additions and terminations, and provide updated Eligibility Files to Provider by the fifteenth (15) day of each month during the Term.; and (c) ensure that all Client Materials and Eligibility Files, and provider's use thereof as permitted by this Agreement, complies with all applicable laws, rules, regulations, statutes, case law, ordinances, and Sanctions ("**Applicable Laws**").

4.3 **Subcontractors.** Provider may subcontract its responsibilities to subcontractors subject to agreement terms at least as protective of Client as those contained in this Agreement ("**Subcontractors**"). Provider remains liable for the performance of all Subcontractors as if such Services were performed directly by Provider. Client may use a Solution to access programs, content, and/or services made available by third-parties (each a "**Certified Partner**"). Client acknowledges and agrees that Certified Partners do not constitute Subcontractors, and Provider shall have no responsibility for a Certified Partner's programs or services ("**CP Offering**"). Each Certified Partner is solely responsible for its content, warranties, and for any claims that Client or its Members may have. Provider shall not have any liability under this Agreement relating to the provision of any CP Offering and all such liability is hereby disclaimed. CP Offerings may be subject to these Terms and to any applicable end user license agreement, terms of use, or similar agreements required by the applicable Certified Partner in connection with the CP Offering ("**CP Terms**"). To the extent these Terms conflict with the applicable CP Terms, the CP Terms shall govern with respect to the CP Offering; *provided, however*, that in no event shall any CP Terms restrict or reduce Client's rights or protections with respect to Client Data or Member Data unless otherwise agreed to in writing by Client.

5. FEES AND EXPENSES; PAYMENTS.

5.1 **Fees.** Client shall pay all fees set forth in the Order Form ("**Fees**") within thirty (30) days of the date of Provider's invoice and all disputed amounts within ten (10) business days of resolution of such dispute; *provided, however*, that Client may only withhold disputed amounts up to twenty (20%) percent of any single invoice. Any undisputed amounts shall accrue interest at a rate equal to the greater of: (i) one and a half percent (1.5%) per month, or (ii) the highest rate permitted by Law, whichever is lower. Client agrees to pay all amounts due without any setoff, deduction, or withholding for any reason. If Provider does not receive payment of any sum due to it within thirty (30) days of the invoice, Provider reserves the right to suspend access to the Solution, including but not limited to the Members' ability to accrue or redeem any rewards, until such time as the default has been cured to Provider's satisfaction. Notwithstanding anything to the contrary herein, all invoiced amounts for rewards are due and payable within thirty (30) days of the date of Provider's invoice.

5.2 **Taxes.** Prices do not include any sales, use, excise, transaction, or other similar taxes. All taxes, excluding taxes based on Provider's income or revenues shall be billed to and paid by Client. To the extent such statutory taxes are not included in an invoice and are later determined to be due, Provider will notify and separately invoice for taxes and the Client will be responsible for payment. Client will make all required payments to Provider free and clear of, and without reduction for, any withholding taxes. Any such taxes imposed on payments to Provider will be Client's sole responsibility, and Client will, upon Provider's request, provide Provider with official receipts issued by the appropriate taxing authorities, or such other evidence as Provider may reasonably request, to establish that such taxes have been paid. Provider shall, upon written request of Client, furnish statements of taxes

and assessments for which Client is responsible and Provider has paid.

5.3 **Invoicing**. Unless otherwise specified on the applicable Order Form or SOW : (a) Fees recurring for use of the Solutions or any Selected Services Fees shall commence upon the earlier of (i) the date on which Provider will make the Solution available to the participating Eligibles ("Initial Order Start Date"), or (ii) one hundred and twenty (120) days following the Effective Date; and (b) all Fees for implementation and configuration Services ("Implementation Services Fee") shall commence on the Effective Date.

5.4 **Renewal Increases to Fees.** In the event an initial committed Term is set forth in an Order Form (the "**Initial Term**") and such Order Form renews for additional terms (each, a "**Renewal Term**" and together with the Initial Term, including the Term), Client agrees that the following standard renewal rates shall apply unless specified otherwise in the Order Form:

a. 3-year renewal - 3% increase to Subscription Fees;

b. 2-year renewal - 5% increase to Subscription Fees; and

c. 1-year renewal - 7.5% increase to Subscription Fees (each, a "**Renewal Term**").

Each Order Form will automatically renew for a period of one (1) year in accordance with Section 5.3(c) at the end of the then-current Term unless either Party provides written notice of non-renewal at least one hundred twenty (120) days prior to the expiration of the then-current Term.

5.5. **Rewards.** In the event that any Member earns and otherwise accrues an entitlement to an incentive but such Member's participation in the Solutions is terminated by the Member and/or the Client, then such Member shall have a period of thirty (30) days following the date of such termination to redeem the applicable Incentive. If the Member fails to redeem the incentive by such date (the "Expiration Date"), then Provider shall be entitled to retain all such unredeemed amounts ("**Forfeited Incentives**") in consideration of its administration of the rewards and incentive program in lieu of charging any administration fee or service charge. Client expressly acknowledges and agrees that the amount for Forfeited Incentives does not constitute a penalty of any kind but rather is an equitable allocation of the cost of incentive administration.

5.6 **Audits.** Provider shall maintain records in accordance generally accepted accounting principles and practices and in accordance with statutory requirements and Applicable Laws. During the Term, Client shall have the right to audit books and records at its own expense to substantiate Provider's Fees ("**Fee Audit**") and Provider will reimburse Client for any expenses incurred by Client in connection with any Fee Audit that results in the correction of a billing error by Provider in an amount greater than ten percent (10%). In addition, Client shall be entitled to perform, at its own expense, an audit to verify Provider's compliance with the Security Controls ("**Security Audit**"); provided, however that if the subject of the Security Audit is covered by an industry-standard assessment by an accredited third-party ("**Third-Party Assessment**"), Client agrees to limit the scope of its Security Audit only to a short questionnaire of no more than thirty (30) questions addressing legitimate concerns not covered by such Third Party Assessment ("**Gap Questionnaire**"). If Provider is in the process of a Third-Party Assessment, then Client shall not provide such Gap Questionnaire until sixty (60) days after Provider's notification that such Third-Party Assessment is complete. All Third-Party Assessments and gap Questionnaires shall be subject to confidentiality protection and be due upon no less than thirty (30) business days' notice to Provider, and no more than once annually.

6. CONFIDENTIAL INFORMATION.

6.1 **Confidential Obligations** The Parties acknowledge that during the performance of this Agreement, each Party will have access to certain written or oral information disclosed by the other that has been identified as confidential or that or should be known to a reasonable person given the facts and circumstances of the disclosure, as being confidential or proprietary ("**Confidential Information**"). The Parties agree to treat and maintain as confidential and proprietary all Confidential Information furnished by the other Party pursuant to or in connection with this Agreement and an Order Form to the same extent and with the same degree of care as it uses in handling its own confidential and proprietary information of similar nature (but with not less than a reasonable degree of care), and further agree not to use such Confidential Information for any purpose other than the performance of any obligation under this Agreement or an Order Form. Neither Party shall disclose any Confidential Information to anyone other than each Party's respective employees or its legal counsel, auditors, agents or consultants (collectively, "Representatives") who are subject to appropriate confidentiality policies or are bound by appropriate confidentiality agreements with terms at least as protective as the terms set forth in this Section 6 and who have a need to know the Confidential Information.

6.2 **Confidentiality Exceptions**. Notwithstanding the foregoing, Section 6.2 will not apply to Confidential Information that (a) is publicly available or in the public domain at the time disclosed; (b) is or becomes publicly available or enters the public domain through no fault of the recipient; (c) is rightfully communicated to the recipient by persons not bound by confidentiality obligations with respect thereto; (d) is already in the recipient's possession free of any confidentiality obligations with respect thereto at the time of disclosure; (e) is independently developed by the recipient; or (f) is approved for release or disclosure by the disclosing Party without restriction; (f) consists of any comments, commentary on any new features, functionality or improvements for Products and/or error reports provided by Client to Provider, provided that such use shall not identify Client ("**Feedback**"); or (g) constitutes De-Identified Data. Either Party may disclose Confidential Information to the limited extent required to establish such Party's rights under this Agreement, including to make such court filings as it may be required to do, or comply with the order of a court or other governmental body or applicable law, provided that the Party making the disclosure pursuant to the order shall first have given written notice to the other Party and make a reasonable effort to obtain a protective order. Client agrees that it will not assert any limitations to Provider's right to use the Feedback or entitlement to compensation or recognition for Provider's use of the Feedback.

6.3 **Location.** Provider shall store all Client Data in accordance with the Data Security Standards and Business Associate Agreement attached as Appendices C and D of this Agreement ("**Security Policies**") and all Applicable Laws, including HIPAA; *provided, however*, that Provider may permit persons physically located outside of the United States ("**Offshore Resource**") to access Client Data (including Protected Health Information ("**PHI**")) and Member Data where: (a) access to Client Data and Member Data is strictly limited to connection via virtual desktop infrastructure ("**VDI**") provided, monitored, and maintained by Virgin Pulse/Provider within the United States ("Secure Remote Worker Application"); (b) each offshore resources is employed directly by Provider at a location owned or operated by Provider or by a U.S. Based Subcontractor that is subject to and compliant with HIPAA and regulations promulgated by the U.S. Department of Health and Human Services, and for the acts and omissions of which Provider remains liable; and (c) Provider ensures that any computer used by Offshore Resources to remotely access Secure Remote Worker Application via the VDI is technically restricted from simultaneously accessing the Internet or using any virtual private network or any other third party

network while logged on to the VDI; and (d) the VDI prevents downloading, printing, extracting, storing or transmitting the information and/or data through personally owned, rented, or borrowed equipment, including but not limited to, laptops, personal digital assistants, instant messaging devices, Universal Serial Bus ("**USB**") devices, and cell phones. Client acknowledges and agrees that in the event Client prohibits use of an Offshore Resource that complies with the forgoing conditions, such withholding or delay shall excuse Provider from any delay in meeting resolution service level agreements associated with any issue, defect, or break for which an Offshore Resource was offered and may result in an increase to the applicable Fees.

7. REPRESENTATIONS, WARRANTIES, AND DISCLAIMERS.

7.1 **Representations; Warranties.** Each Party hereby represents and warrants (a) that it is duly organized, validly existing and in good standing under the laws of its jurisdiction of incorporation or organization; (b) the execution and performance of this Agreement will not conflict with or violate any Applicable Law; and (c) that this Agreement, when executed and delivered, will constitute a valid and binding obligation of such Party and will be enforceable against such Party in accordance with its terms.

7.2 **By Provider.** Provider represents and warrants to Client that: (a) it is the owner and/or the licensee of all IP Rights relating to the Solutions (excluding any Client Materials included therein) and has the necessary rights to grant all licenses hereunder; (b) the Solutions shall perform in compliance with the product descriptions listed in the Order Form; (c) it shall perform the Services in a professional and workmanlike manner in accordance with Applicable Laws; and (d) it shall promptly report to Client any revocations of consent or opt-outs that it receives.

7.3 **By Client.** Client represents and warrants: (a) that it shall not provide any individual social security number, unique national identifier or tax number; (b) that it shall use Provider Data in accordance with this Agreement; (c) that it is solely responsible for the wellness program design, inclusive of incentive structure; (d) that it will comply with all Applicable Laws, including in connection with: (i) its use and design of any custom questions added to Client's HRA or Client designed and built custom Surveys and (ii) obtaining and maintaining in effect all consents required by the Telephone Consumer Protection Act ("TCPA") and the Health Insurance Portability and Accountability Act of 1996 as amended ("HIPAA") to allow Provider to host and process Client Data and/or to authorize Provider to send SMS or pre-recorded messages using an autodialer ("Calls") on Client's behalf and promptly reporting to Provider any revocations of consent or opt-outs it receives; and (d) it will not use the Solution for as a replacement for medical services or other critical uses where the failure or the potential failure of the Services can cause injury, harm or death.

7.4 **Exclusive Warranties; Disclaimer of Warranties**. THE WARRANTIES CONTAINED IN THIS SECTION 7 CONSTITUTE THE EXCLUSIVE WARRANTIES MADE BY PROVIDER AND, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, PROVIDER EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES., EXPRESS OR IMPLIED. EXCEPT AS SET FORTH IN THIS SECTION 7, ALL SOLUTIONS AND SERVICES ARE PROVIDED "AS IS," "WHERE IS" AND "AS AVAILABLE" AND PROVIDER DOES NOT WARRANT THAT THE SOLUTIONS OR SERVICES WILL MEET CLIENT'S REQUIREMENTS OR WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL ERRORS WILL BE CORRECTED. PROVIDER IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM USE OF THE INTERNET. PROVIDER MAKES NO REPRESENTATION AS TO THE VERACITY OF ANY MEMBER DATA. PROVIDER EXPRESSLY DISCLAIMS ANY AND ALL LIABILITY FOR ANY CP OFFERING. THE PARTIES AGREE THAT PROVIDER IS NOT A CARE PROVIDER AND DOES NOT PROVIDE DIAGNOSTIC SERVICES OR MEDICAL ADVICE. THE SOLUTIONS, SERVICES AND CONTENT ARE NOT INTENDED TO BE A SUBSTITUTE FOR ANY MEDICAL EVALUATION, EXAMINATION, ADVICE, DIAGNOSIS OR TREATMENT. FURTHER, THE CONTENT PROVIDED THROUGH THE SERVICES IS NOT MEDICAL ADVICE, IS FOR INFORMATIONAL PURPOSES ONLY AND IS INTENTED TO PROVIDE BROAD USER UNDERSTANDING OF VARIOUS HEALTH-RELATED TOPICS. THE PARTIES HEREBY IRREVOCABLY DISCLAIM AND OPT-OUT OF ALL APPLICABLE PROVISIONS OF THE UNIFORM COMMERCIAL CODE, THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT AND ANY OTHER LAW THE PROVISIONS OF WHICH ARE IMPLIED IF NOT DISCLAIMED OR OPTED-OUT OF BY THE PARTIES.

8. INDEMNIFICATION.

8.1 **By Provider.** Provider agrees to indemnify, defend, release, and hold harmless Client, and its directors, officers, employees, and agents ("**Related Parties**") from and against any and all losses, liabilities, costs (including reasonable attorneys' fees) or damages directly resulting from any claim by any third party ("**Losses**") arising out of or related to (a) any claim that any Solution or Provider's provision of any Services infringes any third party's IP Rights (a "**Infringement Claim**"); or (b) an unauthorized disclosure or access to PHI stored on Provider's systems ("**Incident Claim**"). Provider will not be liable for an Infringement Claim based on (i) modification(s) made to the Solution by Client; or (ii) use or combination of the Solution with non-Provider programs. In the event of an Infringement Claim, Provider may, at its option, either (A) obtain for Client, at no additional cost, the right to continue to use the Solution or receive the Services, (B) replace or modify the Solution or Services to eliminate the Infringement Claim, or (C) terminate the applicable Order Form and refund to Client any pre-paid but unused Fees paid for the Solution or Services. THIS SECTION STATES PROVIDER'S ENTIRE OBLIGATION AND LIABILITY WITH RESPECT TO ANY INFRINGEMENT CLAIM OR INCIDENT CLAIM.

8.2 **By Client.** Client agrees to hold harmless, indemnify, release, and defend Provider from and against any Losses, arising out of or related to: (a) Client's breach of any Applicable Law, (b) data sharing with Client vendors at the direction of Client; (c) the Client Data; (d) Client's use or mis-use of Client administrative tools, including but not limited to VP Live Pro, or (e) any failure by Client to obtain any consents required under the TCPA.

8.3 **Procedure.** The party seeking indemnification (the "Indemnified Party") shall provide the party obligated to provide such indemnification (the "Indemnifying Party") with: (a) prompt written notification of the claim; (b) sole control and authority over the defense or settlement of the claim; and (c) reasonable assistance. The Indemnifying Party may settle the claim provided that if any settlement requires any action or admission by the Indemnified Party other than payment of money, the Indemnifying Party shall obtain Indemnified Party's prior written consent. Failure by the Indemnified Party to provide prompt notice of a claim shall not relieve the Indemnifying Party of its obligations unless such failure or delay materially prejudices the defense of the claim. The Indemnified Party will have the right, at its option, to defend itself against any such claim or to participate in the defense thereof by counsel of its own choice at its own expense.

9. LIMITATION OF LIABILITY

9.1 DIRECT DAMAGES ONLY. NEITHER PARTY SHALL BE LIABLE TO THE OTHER, OR TO ANY OTHER PERSON, FOR ANY

SPECIAL, EXEMPLARY, INDIRECT, PUNITIVE, INCIDENTAL, RELIANCE, OR CONSEQUENTIAL DAMAGES, INCLUDING ANY DAMAGES RESULTING FROM LOSS OF USE OF DATA OR THE SERVICES, LOST BUSINESS, LOSS OF GOODWILL, LOST REVENUES, FAILURE TO REALIZE ANTICIPATED SAVINGS, OR LOST PROFITS, AND ANY OTHER DAMAGES FOR ECONOMIC LOSS ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE INSTALLATION, IMPLEMENTATION, CUSTOMIZATION, USE, INABILITY TO USE, OPERATION OR SUPPORT OF THE SERVICES.

9.2 MAXIMUM LIABILITY. WITH THE EXCEPTION OF CLIENT'S PAYMENT OBLIGATIONS, EACH PARTY'S MAXIMUM AGGREGATE LIABILITY TO THE OTHER OR TO ANY OTHER PERSON FOR ANY LOSS ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE INSTALLATION, IMPLEMENTATION, CUSTOMIZATION, USE, INABILITY TO USE, OPERATION OR SUPPORT OF THE SOLUTION OR SERVICES SHALLL NOT EXCEED THE TOTAL FEES PAID AND/OR PAYABLE BY CLIENT IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT(S) GIVING RISE TO SUCH LIABILITY. NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS OF LIABILITY SET FORTH IN SECTION 9.2 SHALL NOT APPLY TO LIABILITY OF EITHER PARTY RELATED TO SUCH PARTY'S OBLIGATION OF INDEMNIFICATION, WHICH LIABILITY SHALL BE LIMITED IN THE AGGREGATE OVER THE ENTIRE TERM OF THIS AGREEMENT TO FIVE MILLION DOLLARS ($5 MILLION).

9.3 ESSENTIAL PURPOSE. TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE PROVISIONS SET FORTH IN THIS SECTION 9 SHALL APPLY REGARDLESS OF THE FORM OR ACTION OR THEORY OF LIABILITY AND EVEN IF A PARTY WAS ADVISED OF THE POSSIBILITY OF DAMAGES AND WHETHER DAMAGES WERE REASONABLY FORESEEABLE. THE PARTIES AGREE THAT THESE LIMITATIONS ARE ESSENTIAL COMPONENTS OF THIS AGREEMENT AND FORM THE BASIS FOR DETERMINING THE FEES CHARGED FOR THE SERVICES, AND THAT PROVIDER WOULD NOT ENTER INTO THIS AGREEMENT WITHOUT THESE LIMITATIONS ON ITS LIABILITY. THESE LIMITATIONS WILL APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO FAIL OF ITS ESSENTIAL PURPOSE.

10. GENERAL.

10.1 Independent Contractors. In making and performing this Agreement, Client and Provider act and will act at all times as independent contractors, and, except as expressly set forth herein, nothing contained in this Agreement will be construed or implied to create an agency, partnership or employer and employee relationship between them. Except as expressly set forth herein, at no time will either Party make commitments or incur any charges or expenses for, or in the name of, the other Party.

10.2 Notices. All notices required by or relating to this Agreement will be in writing and will be sent by means of certified mail, postage prepaid, to the Parties at their respective addresses set forth in the Order Form or addressed to such other address as the receiving Party may have given by written notice in accordance with this provision. All notices required by or relating to this Agreement may also be communicated by electronic communications provided that the sender receives and retains confirmation of successful transmittal to the recipient. Such notices will be effective on the date indicated in such confirmation.

10.3 Assignment; Delegation. Except in the case of merger, acquisition or sale of all, or substantially all, of a party's assets or capital stock, neither Party shall assign any of its rights or delegate any of its duties under this Agreement without the express, prior written consent of the other Party, and, absent such consent, any attempted assignment or delegation will be null, void and of no effect.

10.4 Third-Party Beneficiaries. The terms and conditions of this Agreement shall be incorporated by reference into any Order Form placed by Client for a Certified Partner program and the Certified Partner and Client shall be a third-party beneficiary to that Order Form. Except for Certified Partners under an Order Form, there are no third-party beneficiaries to this Agreement, expressed or implied.

10.5 Force Majeure. Except with respect to payment obligations hereunder, if a Party is prevented or delayed in performance of its obligations hereunder as a result of circumstances beyond such Party's reasonable control, including, by way of example, Internet access outside of Provider's control, war, terror, riot, fires, floods, epidemics, or failure of public utilities or public transportation systems, such failure or delay will not be deemed to constitute a material breach of this Agreement, but such obligation will remain in full force and effect, and will be performed or satisfied as soon as reasonably practicable after the termination of the relevant circumstances causing such failure or delay, provided that if such Party is prevented or delayed from performing for more than ninety (90) days, the other Party may terminate this Agreement upon thirty (30) days' written notice.

10.6 Governing Law. This Agreement shall be governed by the laws of the State of Rhode Island (except for any conflicts-of-law principles of such state that would result in the application of the law of another State). Any legal action brought under or in connection with this Agreement shall be brought only in the United States District Court or the State Court sitting in the Rhode Island. Each Party waives any objection to such venue and agrees not to claim that any action has been brought in an inconvenient forum.

10.7 Dispute Resolution. Prior to the initiation of any litigation, a Party will provide written notice describing the dispute in reasonable detail and the Parties will use good faith efforts to resolve their dispute informally for sixty (60) days. The Parties will use good faith efforts to arrange personal meetings and/or telephone conferences as needed with representatives with the authority to resolve the dispute. However, after such sixty (60) day period, if the dispute has not been resolved, either party may litigation proceedings.

10.8 Injunctive Relief. The Parties acknowledges that misuses or disclosure of the other Party's Confidential Information (or violation of other proprietary data rights) may give rise to irreparable injury to the other Party that is inadequately compensable in damages. Accordingly, either Party may seek and obtain injunctive relief against the breach or threatened breach of Confidential Information, pending resolution of any dispute and/or in addition to any other legal remedies that may be available. Each Party acknowledges and agrees that the covenants contained in this Section are necessary for the projection of legitimate business interest of the Parties and are reasonable in scope and content.

10.9 U.S. Government End-Users. If Client is part of any agency, department, or other entity of the United States Government ("**U.S. Government**") or is acquiring the Services under a U.S. Government contract, the use, duplication, reproduction, release, modification, disclosure or transfer of the Services, and any other Provider's Confidential Information, is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. The Services are a "commercial item," "commercial computer software" and "commercial computer software documentation." In accordance with such provisions, any use of the Services by the U.S. Government will be governed solely by the terms of this Agreement.

10.10 Miscellaneous. This Agreement, as executed by the Parties, constitutes the entire Agreement of the Parties with respect to its subject matter and supersedes any and all oral or written representations, understandings, or agreements relating thereto. This Agreement has been drafted jointly by the Parties and any ambiguities shall not be construed in favor of or against either Party. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which shall constitute one and the same instrument. This Agreement may be modified only by an agreement in writing that is signed by both Provider and Client. In the event of a conflict among the documents composing this Agreement, the order of precedence and control will be: (i) this Agreement; (ii) the Order Form; and (iii) the Change Order. If any provision of this Agreement is found to be unenforceable by a court of law, the parties shall negotiate in good faith to agree upon a substitute provision that is consistent with the intentions underlying the original provision and the remainder shall be enforced to the extent permitted by Law. No waiver will be valid unless in writing and signed by the Party against which such waiver is sought to be enforced. The waiver or failure of either Party to exercise any right will not be deemed a waiver of any future right**.** The following Sections of these Terms shall survive termination or expiration of the Agreement for any reason: 3, 5, 6, 7, 8, 9 and 10.

APPENDIX C: VIRGIN PULSE DATA SECURITY STANDARDS

1. **Scope; Definitions:** Provider shall comply with the requirements set forth in this Appendix. This Appendix relates to Services whereby Provider collects, accesses, processes, stores, transfers, transmits, uses, discloses, or otherwise handles any Personal Data. In the event of a conflict or inconsistency between any provision of this Appendix and the Agreement, the more stringent requirement shall prevail. Capitalized terms in this Appendix not herein defined are defined in the Agreement or have the following meanings:
"**Agreement**" shall mean the agreement between Client and Provider to which this Appendix is attached.
"**Personal Data**" shall mean, relative to the Services provided to Client, any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; including individually identifiable information contained in Eligibility Files and Member Data, each as defined in the Agreement.
"**PII"** shall mean information (i) that identifies an individual, (ii) with respect to which there is a reasonable basis to believe the information can be used to identify an individual, or (iii) is considered personally identifiable information by applicable codes, laws, guidelines, rules or regulations, including, without limitation, industry self-regulation. The term PII shall also include any "Personal Data" as defined in the General Data Protection Regulation (Regulation (EU) 2016/679).
"**Provider**" shall have the meaning outlined in Provision 1.20 of the Agreement.
"**Provider Personnel**" shall mean each director, officer, manager, employee, representative and each natural person employed or retained by Virgin Pulse.
"**Provider Sites**" shall mean locations owned or leased by Provider from which it provides services to its Clients.
"**Security Incident**" shall mean any confirmed unauthorized access, disclosure, misappropriation, theft, loss, acquisition, or use of Personal Data.
"**Services**" shall mean the services to be provided and performed by Provider pursuant to the Agreement.
"**Systems**" shall mean hardware, software, networks, applications and other equipment that comprise a technical environment used to store or process Personal Data.
"**Industry Standard Security Practices**" shall mean the core security practices appropriate to the Provider's business and services which are commonly implemented as standards across the information technology industry. For example, many of the authoritative sources listed in the HITRUST CSF, ISO-27001, SOC2 and NIST CSF.
"**Security Policies**" shall mean Provider's policies for securing information or data according to Industry Standard Security Practices and in compliance with applicable laws and regulations. Typically, Security Policies are high level instructions to management on how the organization is to be run with respect to Industry Standard Security Practices.
"**User**" shall mean Provider Personnel authorized by Provider to access Personal Data stored on any Provider Systems.

2. **Information Security Program:** Provider has established and, during the term of the Agreement, will maintain:
An ongoing program of Security Policies and controls that comply with the HITRUST Common Security Framework, ISO-27001, SOC2, or similar Industry Standard Security Practices.
A Security Incident management program intended to detect and respond to Security Incidents.
A security awareness and training program that includes both User and administrator training in methods, procedures, and security.
A Business Continuity / Disaster Recovery (BCDR) program in place for critical systems used for storing, transmitting, or processing Personal Data or used for business-to-business communications that includes documented policies and plans, and must test that plan at least annually.
Change control procedures for any Systems Provider uses to store, transmit, transfer, or process Personal Data for Client.
Procedures to conduct periodic independent security risk evaluations and penetration tests to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for timely remediation for Provider's key Systems used to deliver the Services.
A vulnerability management program to assess and manage threats to the Provider's Systems with timely remediation of issues found.

3. **Physical Access:** Provider has established and, during the term of the Agreement, will maintain:
Physical controls to protect Personal Data stored in any Provider data center.
Appropriate facility entry controls are in place to limit physical access to systems that store or process data.
Processes to block access to facilities by default and only grant such access on a "need to know" basis.
Processes to monitor access to any facility where Provider processes Personal Data.

Controls to physically secure all Personal Data and to properly destroy such information when no longer needed using a process equal to or above that specified by NIST Special Publication 800–88, Guidelines for Media Sanitization, such that the Information cannot be retrieved.

Procedures to store securely hardcopy documents, removable media or portable devices containing Personal Data where access is limited to a need-to-know basis. Provider

Procedures to ship physical copies of Personal Data, when required to do so under the Agreement, using secure, reputable shipping services with shipment tracking and confirmed deliver options.

4. **Logical Access:** Provider, with respect to the internal systems used to support the Services, has established and, during the term of the Agreement, will maintain:
   a. Appropriate mechanisms for User authentication and authorization in accordance with a restricted "need to know" and "principle of least privilege" policy, including restrictions on copies and backup copies of all Personal Data.
   b. Procedures to remove or update User access when a User's role changes or terminates.
   c. Procedures to monitor and review User access to validate that User access grants are in line with their current roles.
   d. Multi-Factor authentication for any remote Users or internet facing applications, User portals, User VPN's, virtual desktops or similar internet facing exposures.
   e. Controls to enforce access restrictions for remote Users, contractors, and service providers.
   f. Timely and accurate administration of User account and authentication management.
   g. Processes to assign unique IDs to each User with computer access and limit use to such User.
   h. Processes to change any vendor supplied defaults for passwords and security parameters for Systems prior to deployment.
   i. Controls to validate that User passwords meet minimum length and complexity requirements, and are appropriately changed, managed, and maintained on a regular basis consistent with Industry Standard Security Practices.
   j. Mechanisms to track all access to Personal Data by unique ID to individual Users, and recording the date, time, individual, and nature of the access in a log file, such log files to be kept for a minimum of 1 year.
   k. Mechanisms to encrypt or hash all passwords in storage.
   l. Processes to immediately revoke accesses of inactive accounts or terminated/transferred Users in a timely manner, not to exceed 24 hours.
   m. Controls to restrict copy and paste functions or any other method of information disclosure to the minimum necessary to provide the Services.

5. **Subcontractors and Third Parties:**

   When Provider engages a subcontractor to store, collect, or process Personal Data, Provider will enter into an agreement with such subcontractor that includes data protection terms and provisions substantially similar to those contained in this Appendix.

   When Client directs Provider to exchange Personal Data with, or otherwise collaborate with, a third party in relation to the Services, Client will be responsible for enforcing relevant data protection terms against such third party and Provider will be entitled to rely on Client to conduct any relevant security assessment.

6. **Background Checks and Screening:** Prior to the start of employment, Provider shall conduct, or require a relevant third party to conduct, criminal background checks on Provider Personnel, in alignment with Industry Standard Security Practices.

7. **Security Architecture and Design:** Provider has established and, during the term of the Agreement, will maintain:

   A security architecture designed to support Industry Standard Security Practices.

   Documented and enforced technology configuration standards.

   Processes to encrypt Personal Data, including all backup copies of the same, in transmission and in storage, including storage on any portable media when such media is required to perform the Services, using current industry standard methods (AES 256bit or higher).

   Processes for regular testing of security systems and processes on an annual basis or more frequently as appropriate.

   A system of effective firewall(s) and intrusion detection technologies to protect Personal Data.

   Database and application layer design processes that include data protection requirements to protect Personal Data that is collected, processed, and transmitted through such systems.

   Procedures to backup critical systems that contain Personal Data no less frequently than weekly.

8. **System and Network Management:** Provider has established, and during the term of the Agreement, will maintain:

   Mechanisms to keep Systems security patches current by installing all high risk or higher patches as soon as they can safely be installed but in any event within 90 days from learning about the patch.

   Processes to monitor, analyze, and respond to security alerts issued by hardware and software vendors.

   Appropriate network security design elements that provide for segregation of data.

Anti-virus and malware detection software on all Systems processing Personal Data to protect against malicious software, or processes in place to scan on at least a daily basis.
Appropriate data loss prevention (DLP) controls to protect Personal Data;
Processes to regularly verify the integrity of installed software and determine if any compromise of Personal Data.
Documented change control process to manage all changes to Systems.

9. **Security Incident Notification:** Provider will be responsible for detecting and responding to Security Incidents. Upon becoming aware of a Security Incident, Provider will report such Security Incident within seventy-two (72) hours by providing a written notification to the Client. In the event of a Security Incident, (a) Provider will cooperate with Client to comply with any legal requirement to notify individuals whose Personal Data has been or may have been compromised as a result of a Security Incident; provided that in no event will Provider serve any notice or otherwise publicize a Security Incident without the prior written consent of Client, unless required by applicable laws, and (b) upon Client's request, engage a mutually acceptable, regionally recognized third party to perform or assist with forensic analysis. Provider will deliver the results of any such analysis to Client in accordance with the confidentiality and notice provisions of the Agreement.

10. **Right to Audit:** Provider agrees to provide, upon written request, written attestation or third-party certification of Provider's compliance with industry standard security framework audits such as HITRUST, ISO-27001, SOC 2, PCI-DSS, NIST sp800-53, or similar as validation of Provider compliance with this DSE on an annual basis, or as reasonably required in response to a Security Incident involving Provider or provided service(s). In the event Provider is unable to produce the forms of validation as indicated above, then Provider agrees to submit to the Client the organization's SIG to address any Client risk assessment questions.

11. **Compliance with Law:** Provider complies with all applicable international, federal, state, and local data protection laws and regulations.

12. **Termination:** Upon any termination of the Agreement, Provider will promptly delete any Personal Data, within 90 days of the termination date.

APPENDIX D: BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("**BAA**") is entered into by and between **Fort Bend County, TX**, on behalf of itself or on behalf of its group health plans as applicable (collectively "**Covered Entity**") and Virgin Pulse, Inc. with an address at 75 Fountain Street, Suite 310, Providence, RI 02902, on behalf of itself and its affiliates ("**Business Associate**") (collectively, the "Parties" or individually, a "Party").

Whereas Business Associate renders wellness services to Covered Entity under an existing written agreement (the "**Agreement**"), that may involve the use, disclosure and/or creation of certain Protected Health Information ("**PHI**"), as defined below; and

Whereas, the Parties desire to protect the privacy and security of PHI in compliance with (i) the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") as amended by the Health Information Technology for Clinical Health ("HITECH") Act, Title XIII of Division A and Title IV Division B of the American Recovery and Reinvestment Act of 2009, as set forth in Title 45, Parts 160, 162 and 164 of the Code of Federal Regulations ("**CFR**"), in each case only as of its applicable compliance date (the "**Omnibus Regulations**") that apply to covered entities and business associates; and (ii) the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Part 160, Part 162, and Part 164, as further amended from time to time ("**HIPAA Rules**").

Now, therefore the Parties agree as follows:

1. Term. Subject to Section 19, the term of this BAA ("**Term**") shall be coterminous with the Agreement. This BAA supersedes and replaces any other agreement previously put in place between the Parties governing PHI.

2. Termination. Without limiting any other rights of the Parties, if either Party materially fails to adhere to its obligations under this BAA, the other Party may terminate this BAA if such failure is not cured within thirty (30) calendar days to the reasonable satisfaction of the other party. This BAA will automatically terminate unpon termination or expiration of the Agreement.

3. Definitions. Capitalized terms not otherwise defined, and the following terms used in this BAA shall have the meanings ascribed in 45 CFR Parts 160-164 and are incorporated herein by reference: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. "PHI" and "Electronic Protected Health Information" ("**Electronic PHI**") shall have the same meaning given to such terms in the HIPAA Rules, but limited to such information created or received by Business Associate solely in its capacity as a business associate on behalf of Covered Entity.

4. Use and Disclosure of PHI. Business Associate shall use and/or disclose PHI: (a) only to the extent necessary to perform its duties under the Agreement; (b) to comply with its obligations or as otherwise permitted under this BAA, (c) as required by law and in compliance with each applicable requirement of 45 CFR §164.504(e); and (d) to the extent necessary for Business Associate's proper management and administration. In addition to the uses and disclosures permitted below, Business Associate may also use and disclose PHI: (i) to create a limited data set in accordance with 45 CFR §164.514, which limited data set may be used and disclosed by Business Associate as permitted by law, including HIPAA; (ii) to respond to requests for PHI either accompanied by an authorization that meets the requirements of 45 CFR §164.508 or from a covered entity or health care provider in accordance with 45 CFR §164.506(c) and (iii) as otherwise authorized in writing by Covered Entity or Plan Sponsor on its behalf. In all disclosures, Business Associate shall comply with: (1) the applicable provisions of Title 45, Part 164 of the CFR and (2) applicable State privacy laws, rules and regulations not preempted pursuant to Title 45, Part 160, Subpart B of the CFR or the Employee Retirement Income Security Act of 1974 ("**ERISA**"), as amended. Business Associate may disclose such PHI as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities provided that: (a) the disclosure is required by law (including to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1)); or (b) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person (which purpose must be consistent with the limitations imposed upon Business Associate pursuant to this BAA), and that the person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached

5. Prohibited Disclosures. Business Associate shall not use or disclose PHI other than as permitted or required to perform functions, activities or services for, or on behalf of, Covered Entity as specified in the Agreement or as required by law. To the extent Business Associate is carrying out any of Covered Entity's obligations, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation(s). Business Associate may not use or disclose PHI in a manner that would violate the Privacy Rule if done by Covered Entity, except as set forth in Sections 2(b)-(d).

6. Data Aggregation Services. Business Associate may use and disclose PHI to provide Data Aggregation Services as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

7. De-Identification. Business Associate may create de-identified PHI in accordance with the standards set forth in 45 C.F.R. § 164.514(b) and may use or disclose such de-identified data for any purpose.

8. Safeguards. Business Associate shall use appropriate safeguards, consistent with applicable law including Subpart C of Title 45, Part 164, to prevent the use or disclosure of PHI and ePHI in a manner that would violate this BAA and to reasonably and appropriately protect the confidentiality, integrity and availability of ePHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate shall provide Covered Entity with such information concerning such safeguards as Covered Entity may reasonably request from time to time.

9. Security Incidents. Business Associate shall use commercially reasonable efforts to maintain the security of the PHI and to prevent unauthorized use and disclosures of such PHI. In addition, Business Associate will:

implement Administrative Safeguards, Physical Safeguards and Technical Safeguards, to the extent required of Business Associates by Subpart C of Title 45, Part 164, that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Covered Entity;

report to the Covered Entity any use or disclosure of PHI not provided for by the BAA of which Business Associate becomes aware and any successful Security Incidents that result in the unauthorized access, use, disclosure, modification or destruction of Covered Entity's Electronic Protected Health Information of which Business Associate becomes aware; and

Covered Entity acknowledges that Business Associate may be subject to any number of unsuccessful Security Incidents, such as routine scans or "pings" that do not pass Business Associate's firewall, unsuccessful log-on attempts, denial of service attacks, and any combination of the above (each an "Unsuccessful Security Incident"), as long as such Unsuccessful Security Incident does not result in unauthorized access, Use, Disclosure, destruction or modification of Electronic PHI, Business Associate and Covered Entity agree that this Addendum serves as notice of such Unsuccessful Security Incidents.

10. Breach Notification and Periodic Reports to Plan. Business Associate shall report to Covered Entity any use or disclosure of PHI not permitted under this BAA, Breach of Unsecured PHI or Security Incident, without unreasonable delay, and in any event no more than ten (10) business days following discovery; provided, however, that the Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which notice to Covered Entity by Business Associate shall be required only upon request. "**Unsuccessful Security Incidents**" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on 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. Business Associate's notification to Covered Entity of a Breach shall include: (a) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired or disclosed during the Breach; and (b) any particulars regarding the Breach that Covered Entity would need to include in its notification, as such particulars are identified in 45 C.F.R. § 164.404. Except for notifications to the Secretary, which must be done by Covered Entity, Business Associate agrees that to the extent the Breach is a result of Business Associate's failure to implement reasonable and appropriate safeguards as required by this BAA, Business Associate will provide the notifications required under 45 CFR 164.404 and 45 CFR 164.406 after reviewing the content of such notifications with Covered Entity, subject to any delay required by law enforcement pursuant to 45 CFR 164.412.

11. Security and Privacy Requirements. Business Associate agrees to comply with Sections 164.308, 164.310, 164.312 and 164.314 of the Omnibus Regulations applicable to Business Associates. The Parties hereto agree that the requirements of the Omnibus Regulations relating to security and privacy that are made applicable to Covered Entities shall also be applicable to Business Associate under the BAA to the extent required by the Omnibus Regulations. Except as expressly provided herein, Business Associate has not assumed any obligations of Covered Entity under the HIPAA Rules.

12. Accounting of Uses or Disclosures. Business Associate agrees to provide to Covered Entity, within twenty (20) business days of Business Associate's receipt of a written request from Covered Entity, information collected in accordance with Section 3(f) of this BAA, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. If an Individual makes a request for an accounting of disclosures of PHI pursuant to 45 C.F.R. § 164.528 directly to Business Associate, or inquires about his or her right to an accounting of disclosures of PHI, Business Associate shall direct the Individual to Covered Entity.

13. Access by Workforce. Business Associate agrees to require its Workforce who access PHI in performing services to adhere to the restrictions and conditions regarding PHI contained herein to the extent applicable to their job functions. Business Associate will not provide access to PHI to any member of its Workforce unless Business Associate has advised such member of Business Associate's HIPAA obligations and the consequences for violation of these obligations to the extent applicable to their job functions. Business Associate will take reasonably appropriate disciplinary action against any member of its Workforce that uses or discloses PHI in violation of this section, as required by applicable law or regulation.

Disclosures outside of the Workforce. Except as otherwise permitted by applicable law or in this BAA, including but not limited to Sections 5 (Business Associate's Operations), and with respect to disclosures in response to requests by Individuals who invoke their rights under HIPAA as described in this BAA, Business Associate shall not disclose PHI to any other person or entity without the written approval of Covered Entity.

All disclosures. Any use or disclosures of PHI to Business Associate's Workforce or Contracted Third Party(ies) must be limited to the minimum necessary to achieve the purpose for the use or disclosure in accordance with, and subject to, the exceptions in 45 CFR §164.502(b).

14. Access to Records. Upon confirming the identity of an Individual (or an Individual's personal representative and right to access PHI), Business Associate will respond to an Individual's request for access to his or her PHI, or PHI to which the Individual's personal representative is authorized to access, if the request is communicated to Business Associate directly by the Individual. Despite the fact that the request is not made to the Covered Entity, Business Associate will respond to the request with respect to the PHI Business Associate and its Contacted Third Party(ies) maintain in a manner and time frame consistent with requirements specified in 45 CFR § 164.524. In addition, upon receipt of a written request (including fax or email notice) from Covered Entity, Business Associate will, unless the Covered Entity requests otherwise, respond on behalf of the Covered Entity to an Individual's request to invoke a right of access under 45 CFR § 164.524 as if the access request had been communicated to Business Associate directly by the Individual. If Covered Entity requests that Business Associate not respond as provided in the foregoing sentence, then Business Associate will make available for inspection by the Covered Entity, or at the

Covered Entity's direction, by the Individual (or Individual's personal representative), any PHI about the Individual created or received for or from Covered Entity in Business Associate's custody or control so that Covered Entity may satisfy Covered Entity's access obligations under the HIPAA Rules, and, where applicable the HITECH ACT. Business Associate will make such information available in an electronic format, where required by the HITECH Act, or otherwise make and produce copies of the information requested. Notwithstanding anything to the contrary contained in this BAA, Business Associate will only disclose PHI to individuals of Covered Entity's workforce identified by Covered Entity as individuals authorized to receive or access PHI on its behalf. Business Associate may refuse to provide PHI to any request for receipt or access to PHI on behalf of Covered Entity when that request does not come from an individual authorized to receive or access PHI on behalf of Covered Entity. In the event Covered Entity has not identified said authorized individuals, Business Associate may assume, consistent with 45 CFR §164.504(f), that those individuals managing the services provided by Business Associate are authorized to receive or access PHI on Covered Entity's behalf.

15. Amendment of PHI. To the extent Business Associate maintains a Designated Record Set on behalf of Covered Entity, and upon confirming the identity of an Individual (or an Individual's personal representative and right to access PHI), Business Associate will respond to an Individual's (or Individual's personal representative's) request to amend any PHI if the request is communicated to Business Associate directly by the Individual (or Individual's personal representative). Despite the fact that the request is not made to the Covered Entity, Business Associate will respond to the request with respect to the PHI Business Associate and its Contracted Third Party(ies) maintain in a manner and time frame consistent with requirements specified in HIPAA and 45 CFR § 164.526. In addition, upon receipt of written notice (including faxed and emailed notice) from Covered Entity, Business Associate will, unless Covered Entity requests otherwise, respond on behalf of Covered Entity to an Individual's (or Individual's personal representative's) request to amend his or her PHI as if the amendment request had been communicated to Business Associate directly by the Individual. In the event a request for an amendment of PHI conflicts with a record provided by a confident source of truth (such as a healthcare professional or doctor), Business Associate may require the Individual (or Individual's personal representative) to request an amendment to the PHI through the original source of truth, which must be communicated from said original source of truth directly to Business Associate before Business Associate can amend the PHI.

16. Government Access to Records. Business Associate agrees to make available its policies, books and records related to the use and disclosure of PHI received or created by Business Associate on behalf of the Covered Entity to the Secretary of the U.S. Department of Health and Human Services or his or her designee for the purpose of determining whether Business Associate and/or Covered Entity is in compliance with HIPAA requirements.

17. Disposition of Records upon Termination. Except where Business Associate is required to retain certain PHI for a period of time to comply with applicable laws, Business Associate agrees to destroy all PHI created, maintained or received under this BAA within ninety (90) days of termination of this BAA. If such destruction of records is not feasible, or where Business Associate is required to retain certain PHI by applicable laws, Business Associate will continue to extend the protections of this BAA to such PHI and limit any further use of PHI to those purposes that require Business Associate to retain the PHI under applicable laws and/or purposes that make the destruction of the PHI infeasible. Covered Entity agrees that it is infeasible for Business Associate to destroy PHI reasonably needed to be retained by Business Associate for its own legal and risk management purposes. *provided that all of the PHI provided by the Covered Entity to Business Associate, or created or received by Business Associate on behalf of the Covered Entity, is destroyed , or if it is infeasible to destroy PHI, protections are extended to such information as set forth in Section 19 herein.*

18. Obligations of Covered Entity.

Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR § 164.520, as well as any changes to that notice.

Covered Entity shall promptly provide Business Associate with any changes in, or revocation of, permission by an individual (or an individual's personal representative) to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.

Covered Entity shall notify Business Associate, in writing and in a timely manner, of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522.

Covered Entity acknowledges that it shall provide to, or request from, the Business Associate only the minimum PHI necessary to perform or fulfill a specific function required or permitted hereunder.

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity except as provided herein in accordance with 45 CFR §164.504(e). Covered Entity shall disclose or provide access to Business Associate only the minimum PHI necessary for Business Associate to perform its obligations as required by the Privacy Rule and 42 U.S.C. § 17935(b).

Covered Entity in performing its obligations and exercising its rights under this BAA shall use and disclose PHI in compliance with the HIPAA Rules.

Notwithstanding the above, where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of PHI unless it satisfies the requirements of a valid authorization giving Covered Entity permission to use PHI for purposes other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the individual. If required, Covered Entity acknowledges that it remains responsible for obtaining such consent, authorization or permission that may be required by law or regulation (as opposed to individual consents or authorizations that may be required from plan participants in certain circumstances) for Business Associate to provide its services on behalf of Covered Entity and that Covered Entity shall provide Business Associate with advance written notice of any restrictions or changes to Covered Entity's Notice of Privacy Practices that would limit the uses and disclosures of PHI otherwise permitted

herein. Covered Entity acknowledges that Business Associate shall only be required to comply with such changes to its Notice of Privacy Practices which are known to Business Associate and to the extent required by applicable law or regulation. Covered Entity shall provide to Business Associate a written list of the names of those individuals in its Workforce that are authorized to receive or access PHI on its behalf, and to provide reasonable prior written notice to Business Associate of any changes to such list. In the absence of Covered Entity providing such list, Business Associate may assume, consistent with 45 CFR §164.504(f), that those individuals that are members of the Workforce of Covered Entity who request or receive PHI from Business Associate are performing plan administration activities for Covered Entity, and are authorized to receive or access PHI on its behalf.

19. General. The respective rights and obligations of Business Associate under Section 5(c) of this BAA shall survive the termination of the BAA and the Agreement. In the event of any inconsistency between the provisions of this BAA and the Agreement, the provisions of this BAA shall control. In the event of inconsistency between the provisions of this BAA and mandatory provisions of the Privacy Rule, the Security Rule or the HIPAA Final Rule, or their interpretation by any court or regulatory agency with authority over Business Associate or Covered Entity, such interpretation shall control; provided, however, that if any relevant provision of the Privacy Rule, the Security Rule or the HIPAA Final Rule is amended in a manner that changes the obligations of Business Associate or Covered Entity that are embodied in terms of this BAA, then the Parties agree to negotiate in good faith appropriate non-financial terms or amendments to this BAA to give effect to such revised obligations. Where provisions of this BAA are different from those mandated in the Privacy Rule, the Security Rule, or the HIPAA Final Rule, but are nonetheless permitted by such rules as interpreted by courts or agencies, the provisions of this BAA shall control. This BAA is governed by, and shall be construed in accordance with, the laws of the State that govern the Agreement. If any part of a provision of this BAA is found illegal or unenforceable, it shall be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this BAA shall not be affected. All notices relating to the Parties' legal rights and remedies under this BAA shall be provided in writing to a Party, shall be sent to its address set forth in the signature block below, or to such other address as may be designated by that Party by notice to the sending Party, and shall reference this BAA. This BAA may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of both Parties. Nothing in this BAA shall confer any right, remedy or obligation upon anyone other than Covered Entity and Business Associate. This BAA is the complete and exclusive agreement between the Parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications and understandings (written and oral) regarding its subject matter. Business Associate will be considered, for all purposes, an independent contractor, and Business Associate will not, directly or indirectly, act as agent, servant or employee of Covered Entity or make any commitments or incur any liabilities on behalf of Covered Entity without its express written consent. Nothing in this BAA shall be deemed to create an employment, principal-agent, or partner relationship between the parties. Business Associate shall retain sole and absolute discretion in the manner and means of carrying out its activities and responsibilities under this BAA.

IN WITNESS WHEREOF, the Parties have executed this BAA as of the latest date of execution by the Parties.

By: Covered Entity

_____(Signature)

_____(Print Name)

_____(Title)

Date: _____

By: Business Associate: **Virgin Pulse, Inc.**

DocuSigned by:

_____(Signature)

AB4E708AB6CA47B...

Rik Thorbecke (Print Name)

Chief Financial Officer (Title)

Date: 7/27/2023

Approved by: DocuSigned by: Gina Simonelli Baxter

7093A0F155EE445...

APPENDIX E: VIRGIN PULSE OPTIONAL SERVICES

Service/Product	Product/Service Fee	Notes
Single Sign-On	$2,500 per connection $200 per hour – custom integrations	Above ten (10) provided per the Order Form
Verified Form Processing Setup	$1,500 per setup	
Verified Form Processing	$5.00 – standard form $10.00 – nonstandard form	
HRA Processing	$30.00 – Telephonic $25.00 - Paper	
Custom Destination Challenge	$5,000 per challenge	Only applicable once client exceeds their contracted allotment
Additional Configurable Challenge	$1,500 per challenge	Only applicable once client exceeds their contracted allotment
Custom Promoted Healthy Habit Challenge	$500 per challenge	Only applicable once client exceeds their contracted allotment
Custom Data Extract	$200 per hour	For reporting needs beyond standard automated reporting capabilities (i.e., enrollment, incentives, etc.)
Max Buzz	$10.00 PEPY $28.99 per device	
Wireless Health Stations - Desktop	$539 per unit	Bulk order option available
Wireless Health Stations - iPad	$749 per unit	Bulk order option available
Live/Recorded Webinar	15-minutes: $250 30-minutes: $295 60 minutes: $350 Webinar Series: $1,400	Webinar Series is a 4-week series
Concierge Onsite Health Screening	Fingerstick: $55.00 per unit Venipuncture: $60.00 per unit Cotinine only: $47.00 per unit (venipuncture only) CHEM 36 panel: $78.00 per unit	Minimum of 20 participants per event
Concierge Onsite Flu Vaccinations - LabCorp	$40.00 per unit	Minimum of 30 participants per event
Concierge Onsite Flu Vaccinations - Quest	$45.00 per unit	Minimum of 40 participants per event
Health Activation Partner	$35,000	Available in US; UK; AUS; SWZ; SIN
Health & Wellbeing Program Manager	$140,000	Available in US; UK; AUS; SWZ; SIN; BOS
Workplace Health Coach	$130,000 per year – Full time $70,000 per year – Part time	US Only
Health & Wellbeing Specialist	$130,000 per year – Full time $70,000 per year – Part time	Available in US; UK; AUS; SWZ; SIN; BOS
Program Manager: People Manager	$150,000 per year – Full time $75,000 per year – Part time	Available in UK; AUS; SWZ; SIN; BOS
Virgin Pulse Tobacco Cessation Coaching	$215 Per Participant Per Year	
Virgin Pulse Nicotine Replacement Therapy	$58 per one month supply	