Data Security Agreement

This Data Security Agreement ("Agreement"), made effective as of the ___ of _____ 2020 (the "Effective Date") by _____ ("Provider") and Health on Your Time, LLC, a Delaware limited liability company with offices at 73 Arrowood Lane, Orchard Park, New York 14127 ("HOYT") (Provider and HOYT are sometimes collectively referred to herein as the "Parties" and individually as a "Party").

WHEREAS, the Provider offers its services to customers on the HOYT platform (the "Customer" or "Customers") and may receive, create, maintain, use, or disclose personal information, including but not limited to highly sensitive personal information, personal information, or protected health information, in connection with the functions, activities, and services that the Provider performs.

NOW THEREFORE, in view of the premises and in consideration of the agreements and mutual covenants contained herein, the Parties, intending to be legally bound, hereby agree as follows:

1. Definitions. Capitalized terms used herein shall have the meanings set forth in this Section 1.

"**Authorized Employees**" means Provider's employees who have a need to know or otherwise access Personal Information to enable Provider to perform its obligations under this Agreement.

"**Highly Sensitive Personal Information**" means an (i) individual's government-issued identification number (including Social Security number, driver's license number, or state-issued identification number); (ii) financial account number, credit card number, debit card number, or credit report information, with or without any required security code, access code, personal identification number, or password that would permit access to an individual's financial account; or (iii) biometric, genetic, health, medical, or medical insurance data.

"**Personal Information**" means information provided to Provider by or at the direction of Customer, information which is created, maintained, or obtained by Provider on behalf of Customer, or information to which access was provided to Provider by or at the direction of Customer, in the course of Provider's performance of its services to Customer that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, email addresses, and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, user identification and account access credentials or passwords, financial account numbers, credit report information, student information, biometric, health, genetic, medical, or medical insurance data, answers to security questions, and other personal identifiers), in case of both subclauses (i) and (ii), including, without limitation, all Highly Sensitive Personal Information. Customer's business contact information is not by itself deemed to be Personal Information.

"**Protected Health Information**" and/or "**PHI**" means "protected health information" as defined in the HIPAA Rules and, unless the context clearly requires otherwise, each such term means "protected health information", as defined in the HIPAA Rules, that is created, received, maintained, or transmitted by Provider

"**Security Incident**" means (i) any act or omission that compromises either the security, confidentiality, or integrity of Personal Information or PHI or the physical, technical, administrative, or organizational safeguards put in place by Provider, or by HOYT should Provider have access to HOYT's systems, that relate to the protection of the security, confidentiality, or integrity of Personal Information or PHI, or (ii) receipt of a complaint in relation to the privacy and data security practices of Provider or a breach or alleged breach of this Agreement relating to such privacy and data security practices. Without limiting the foregoing, a compromise shall include any unauthorized access to or disclosure or acquisition of Personal Information or PHI.

2. Standard of Care.

(a) Provider acknowledges and agrees that, in the course of its engagement by Customer, Provider may create, receive, maintain, or have access to Personal Information or PHI. Provider shall comply with the terms and conditions set forth in this Agreement in its creation, collection, receipt, transmission, storage, disposal, use, and disclosure of such Personal Information and/or PHI and be responsible for any unauthorized creation, collection, receipt, transmission, access, storage, disposal, use, or disclosure of Personal Information and/or PHI under its control or in its possession by all Authorized Employees.

(b) In recognition of the foregoing, Provider agrees and covenants that it shall:

(i) keep and maintain all Personal Information and PHI in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure;

(ii) not create, collect, receive, access, or use Personal Information and/or PHI in violation of law;

(iii) use and disclose Personal Information and/or PHI solely and exclusively for the purposes for which the Personal Information and/or PHI, or access to it, is provided pursuant to the terms and conditions of this Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Information for Provider's own purposes or for the benefit of anyone other than Customer, in each case, without Customer's prior written consent; and

(iv) not, directly or indirectly, disclose Personal Information and/or PHI to any person other than its Authorized Employees, including any, subcontractors, agents, service providers, or auditors (an "Unauthorized Third Party"), without Customer's prior written consent unless and to the extent required by Government Authorities or as otherwise, to the extent expressly required, by applicable law , in which case, Provider shall (A) use best efforts and to the extent permitted by applicable law notify Customer before such disclosure or as soon thereafter as reasonably possible; (B) be responsible for and remain liable to Customer for the actions and

omissions of such Unauthorized Third Party concerning the treatment of such Personal Information as if they were Provider's own actions and omissions; and (C) require the Unauthorized Third Party that has access to Personal Information and/or PHI to execute a written agreement agreeing to comply with the terms and conditions of this Agreement.

3. Information Security.

(a) Provider represents and warrants that its creation, collection, receipt, access, use, storage, disposal, and disclosure of Personal Information and/or PHI does and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations and directives.

(b) Provider shall implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

(c) Without limiting Provider's obligations under Section 3(a), Provider shall implement administrative, physical, and technical safeguards to protect Personal Information from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices, and shall ensure that all such safeguards, including the manner in which Personal Information and/or PHI is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable federal and state data protection and privacy laws, as well as the terms and conditions of this Agreement.

If, in the course of its engagement by Customer, Provider has access to or will collect, access, use, store, process, dispose of, or disclose credit, debit, or other payment cardholder information, Provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Provider's sole cost and expense.

(d) At a minimum, Provider's safeguards for the protection of Personal Information and/or PHI shall include: (i) limiting access of Personal Information and/or PHI to Authorized Employees; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, application, database, and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) encrypting Highly Sensitive Personal Information stored on any media; (vii) encrypting Highly Sensitive Personal Information transmitted over public or wireless networks; (viii) strictly segregating Personal Information and/or PHI from information of Provider or its other customers so that Personal Information and/or PHI is not commingled with any other types of information; (ix) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Provider's sole cost and expense, a corrective action plan to correct

any issues that are reported as a result of the testing; (x) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (xi) providing appropriate privacy and information security training to Provider's employees.

(e) During the term of each Authorized Employee's employment by Provider, Provider shall at all times cause such Authorized Employees to abide strictly by Provider's obligations under this Agreement. Provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use, or disclosure of Personal Information and/or PHI by any of Provider's officers, partners, principals, employees, agents, or contractors. Upon HOYT's written request, Provider shall promptly identify for HOYT in writing all Authorized Employees as of the date of such request.

4. Security Incident Procedures.

(a) Provider shall:

(i) provide HOYT with the name and contact information for an employee of Provider who shall serve as HOYT's primary security contact and shall be available to assist HOYT twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Incident;

(ii) notify HOYT of a Security Incident as soon as practicable, but no later than twenty-four (24) hours after Provider becomes aware of it; and

(iii) notify HOYT of any Security Incident by emailing HOYT at support@healthonyourtime.com, with a copy by email to Provider's primary business contact within HOYT.

(b) Immediately following Provider's notification to Customer of a Security Incident, the parties shall coordinate with each other to investigate the Security Incident. Provider agrees to fully cooperate with HOYT in HOYT's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing HOYT with physical access to the facilities and operations affected; (iii) facilitating interviews with Provider's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise required by HOYT.

(c) Provider shall at its own expense use best efforts to immediately contain and remedy any Security Incident and prevent any further Security Incident, including, but not limited to taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards. Provider shall reimburse HOYT for all actual costs incurred by HOYT in responding to, and mitigating damages caused by, any Security Incident, including all costs of notice and/or remediation pursuant to Section 4(d).

(d) Provider agrees that it shall not inform any third party of any Security Incident without first obtaining HOYT's prior written consent, other than to inform a complainant

that the matter has been forwarded to HOYT's legal counsel. Further, Provider agrees that HOYT shall have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise in HOYT's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

(e) Provider agrees to maintain and preserve all documents, records, and other data related to any Security Incident.

(f) Provider agrees to fully cooperate at its own expense with HOYT in any litigation, investigation, or other action deemed necessary by HOYT to protect its rights relating to the use, disclosure, protection, and maintenance of Personal Information and/or PHI.

In the event of any Security Incident, Provider shall promptly use its best efforts to prevent a recurrence of any such Security Incident.

5. Oversight of Security Compliance. Upon HOYT's written request, to confirm Provider's compliance with this Agreement, as well as any applicable laws, regulations, and industry standards, Provider grants HOYT or, upon HOYT's election, a third party on HOYT's behalf, permission to perform an assessment, audit, examination, or review of all controls in Provider's physical and/or technical environment in relation to all Personal Information and/or PHI being handled and/or services being provided to HOYT pursuant to this Agreement. Provider shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Personal Information and/or PHI for HOYT pursuant to this Agreement. In addition, upon HOYT's written request, Provider shall provide HOYT with the results of any audit by or on behalf of Provider performed that assesses the effectiveness of Provider's information security program as relevant to the security and confidentiality of Personal Information and/or PHI shared during the course of this Agreement.

6. Return or Destruction of Personal Information. At any time during the term of this Agreement at HOYT's written request or upon the termination or expiration of this Agreement for any reason, Provider shall, and shall instruct all Authorized Employees to, promptly return to HOYT all copies, whether in written, electronic, or other form or media, of Personal Information and/or PHI in its possession or the possession of such Authorized Employees, or securely dispose of all such copies, and certify in writing to HOYT that such Personal Information and/or PHI has been returned to HOYT or disposed of securely. Provider shall comply with all reasonable directions provided by HOYT with respect to the return or disposal of Personal Information and/or PHI.

7. Equitable Relief. Provider acknowledges that any breach of its covenants or obligations set forth in this Section or the Provider's standard policies and procedures, a copy of which have been provided to HOYT may cause HOYT irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, HOYT is entitled to seek equitable relief, including a restraining order,

injunctive relief, specific performance, and any other relief that may be available from any court, in addition to any other remedy to which HOYT may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Agreement to the contrary.

8. Material Breach. Provider's failure to comply with any of the provisions of this Section is a material breach of this Agreement. In such event, HOYT may terminate the Agreement effective immediately upon written notice to the Provider without further liability or obligation to Provider.

9. Indemnification. Provider shall defend, indemnify, and hold harmless HOYT and its subsidiaries, affiliates, and its respective officers, directors, employees, agents, successors, and permitted assigns (each, a "HOYT Indemnitee") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any HOYT Indemnitee arising out of or resulting from Provider's failure to comply with any of its obligations under this Agreement.

[Signature Page Follows]

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date first written above.

Provider:

_____

By:
Title:

Health on Your Time, LLC

_____

Scott Monte, President

[Signature Page to Data Security Agreement]