**WORKFORCE SAFETY SUBSCRIPTION AGREEMENT – AWS MARKETPLACE**

BY ELECTRONICALLY INDICATING TO AMAZON WEB SERVICES THAT YOU WOULD LIKE TO ORDER THE APPIAN WORKFORCE SAFETY APPLICATION, YOU AGREE TO THE FOLLOWING TERMS AND CONDITIONS (“AGREEMENT”). THIS AGREEMENT GOVERNS YOUR USE OF THE WORKFORCE SAFETY SOLUTION AND THE UNDERLYING APPIAN LOW-CODE PLATFORM (COLLECTIVELY, THE “SOLUTION”). IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THIS AGREEMENT, IN WHICH CASE THE TERMS “YOU” OR “YOUR” SHALL REFER TO SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THIS AGREEMENT, YOU MAY NOT USE THE SOLUTION.

This Agreement is effective as of the date You accept this Agreement (“Effective Date”).

Last Updated: 15 August 2020

**1. Appian Entity**. The Appian entity that is a party to this Agreement depends upon Your geographic location, as described in the table below. The applicable Appian legal entity may be referred to in this Agreement as “We”, Us” or “Our”.

|  |  |
| --- | --- |
| Your Location | Applicable Appian Legal Entity |
| If You are located in the United States or Canada | Appian Corporation, located at 7950 Jones Branch Drive, Tysons, Virginia 22102 |
| If You are located outside the United States or Canada | Appian Software International, located at Baarerstrasse 21, 6300 Zug, Switzerland |

**2.  License Grant, Restrictions, and Payment.**

a. General. For a period of one year from the Subscription Start Date, Appian will provide You with a non-exclusive, non-transferable license, without right of sublicense, to access the Solution, via a Username and password over the Internet, subject to the term of this Agreement. You may only use the Solution in connection with Your own internal business purposes related to managing processes and cases related to workforce safety and readiness management. You may not use the Solution to develop any other applications. You must limit access and use of the Solution to a reasonable number of Your employees and contractors who are compliant with this Agreement. You are responsible for Your employees and contractors who violate this Agreement, including all usage by user accounts provisioned by You. You must maintain the confidentiality of Your account and password information, and You must use reasonable efforts to restrict access to Your computers or Your instance of the Appian cloud. In the event of a breach of security, You must immediately change Your passwords and notify Us of such breach. For the purposes of this Agreement, the Subscription Start Date will be the first date after which Your right to cancel Your order of the Solution has expired (i.e., the day after the Amazon Web Services 48-hour window for cancellation has expired).

b. Restrictions. You may not: (i) copy, sell, rent or distribute the Solution, or any part thereof, (ii) operate the Solution, or any part thereof, on a service bureau or shared basis, (iii) reverse engineer or decompile the Solution, (iv) except as authorized in the documentation associated with the Solution, modify, enhance, adapt or prepare any derivative works from the Solution, or any part thereof, or (v) allow, assist or permit a third party to do any of the foregoing.

c. Ownership. The Solution and all intellectual property rights therein are licensed to You, not sold. All rights in the Solution not provided to You under this Agreement are expressly retained by Us and Our licensors. The Solution is a commercial software product pursuant to DFAR Sections 227-7202-1(a), 227.7202-3(a) and 252.227-7013(c) and FAR Sections 12.212 and 52.227-19.

d. Use by Competitors. You may not access the Solution if You are a direct competitor of Us, or for the purposes of providing access to the Solution to a competitor of Ours. In addition, You may not access the Solution for purposes of monitoring its availability, performance or functionality, or for any benchmarking or competitive purposes.

e. Probing. You shall not and shall not allow anyone working on Your behalf to perform any technical security integrity review, penetration test, load test, denial-of-service simulation or vulnerability scan of the Solution without Our prior written consent.

f. Feedback. If when using the Solution You communicate to Us suggestions for improvements, ideas, enhancement requests or other feedback in connection with the Solution (“Feedback”), We shall own all right, title, and interest in and to the same, even if You have designated the Feedback as confidential, and We shall be entitled to use the Feedback without restriction.

g. Payment. You agree that You will pay Amazon Web Services (or allow Amazon Web Services to collect from You) the subscription fees associated with Your appropriate level of subscription to the Solution pursuant to Your agreement with Amazon Web Services. Appian may terminate your access to the Solution if You have selected the wrong level of subscription based on the size of Your organization.  If Appian terminates Your subscription on this basis, Appian will inform you of such termination and invite you to re-subscribe with the appropriate level of subscription to the Solution.

h. Subscription Information. You agree to provide Appian with sufficient and accurate information to support Your subscription, including but not limited to, the total number of employees in Your organization, Your organization’s name and headquarters location, the identity and contact information for Your subscription administrator (the person responsible for administering the Solution in Your organization), and the identity and contact information for person responsible for paying for Your subscription. To the extent that You have provided such information to Amazon Web Services, You consent to Amazon Web Services providing it to Appian.

**3. Confidentiality.**

a. Definitions. A party disclosing Confidential Information to the other party is referred to as the “Discloser”. A party receiving Confidential Information from the other party is referred to as the “Recipient”. “Confidential Information” means any information (i) disclosed in writing by the Discloser to the Recipient and marked confidential, (ii) disclosed orally by the Discloser to the Recipient, identified as Confidential Information at such time, summarized in writing by the Discloser to the Recipient within thirty (30) calendar days of such oral disclosure, (iii) the Solution, and (iv) information and documentation that should be reasonably understood to be confidential under the circumstances of disclosure or the nature of the information disclosed.

b. Restrictions. The Recipient will protect the Confidential Information from unauthorized use and disclosure using the same means it uses to protect its own information and data of like importance, but in no event using less than a reasonable degree of care. The Recipient may only use the Confidential Information as expressly permitted in this Agreement or as otherwise authorized by the Discloser, in writing. The Recipient may only disclose the Confidential Information to its employees, consultants and authorized agents (i) who have a need to know in order for the Recipient to perform this Agreement, and (ii) who are subject to binding confidentiality obligations to the Recipient that are at least as restrictive regarding the limitations on use and disclosure as those in this Section 3. The foregoing restrictions will not apply to information that (I) is properly known by the Recipient at the time of disclosure by the Discloser, (II) has become publicly known through no wrongful act of the Recipient, (III) has been rightfully received by the Recipient from a third party authorized to make such communication without restriction, (IV) has been independently developed by the Recipient without reliance upon the Confidential Information, (V) is required to be disclosed as a matter of law; provided that the Recipient must, to the extent not prohibited by applicable law, give the Discloser sufficient notice of such disclosure to allow the Discloser a reasonable opportunity to object to and to take necessary legal action to prevent such disclosure. The Recipient will promptly notify the Discloser of any unauthorized use or disclosure of the Confidential Information. The Recipient agrees to reasonably assist the Discloser in remedying any such unauthorized use or disclosure.

c, Privacy Obligations. In providing You with the Solution, We shall comply with the privacy obligations set forth in Schedule 1 of this Agreement, which is incorporated herein by reference.

d. Business Associate Addendum. To the extent in the performance of this Agreement You provide Us with Personal Health Information as defined in the Health Insurance Portability and Accountability Act and its implementing regulations (45 C.F.R. Parts 160-164), the Business Associate Addendum set forth in Schedule 2 of this Agreement, and incorporated herein by reference, shall apply.

**4. Disclaimer or Warranty and Liability.**

THE SOLUTION IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EITHER EXPRESS, STATUTORY OR IMPLIED. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE SPECIFICALLY DISCLAIM ANY WARRANTIES IMPLIED BY LAW, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR ANY AND ALL WARRANTIES IMPLIED FROM CUSTOM, USAGE IN TRADE OR COURSE OF DEALING.

IN NO EVENT WILL WE BE LIABLE FOR LOSS OF PROFITS, LOSS OR INACCURACY OF DATA, OR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES. IN ADDITION, EXCEPT IN CONNECTION WITH OUR INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT, IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT DAMAGES IN EXCESS OF THE SUBSCRIPTION FEES PAID TO US AS A PART OF THIS AGREEMENT.

THE SOLUTION MAY CONTAIN FORM QUESTIONNAIRES OR DOCUMENTATION RULES ASSOCIATED WITH RETURN TO WORK ELIGIBILITY.   ANY PRE-LOADED FORMS, RULES AND QUESTIONNAIRES ARE FOR INFORMATION PURPOSES ONLY AND PROVIDED SOLELY TO ACCELERATE YOUR CONFIGURATION OF THE SOLUTION.  YOU ARE SOLELY RESPONSIBLE FOR THE DETERMINATION OF THE APPROPRIATENESS OF THE RETURN TO WORK CRITERIA DEPLOYED IN THE SOLUTION, AND THEIR ADHERENCE TO LOCAL AND NATIONAL LAWS AND REGULATIONS.  THE PRE-LOADED FORMS AND RULES ARE NOT MEDICAL OR LEGAL ADVICE.   YOU AGREES TO INDEMNIFY AND HOLD APPIAN HARMLESS FROM ANY FIRST OR THIRD-PARTY CLAIM BASED ON YOUR USE OF ANY PRE-LOADED RETURN TO WORK FORMS AND RULES IN THE SOLUTION.

THE LIMITATIONS SET FORTH IN THIS SECTION ARE INDEPENDENT OF ANY LIMITED REMEDY SET FORTH HEREIN, SHALL APPLY WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND SHALL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

**5. Maintenance Services** – We shall provide the following services (collectively ‘Maintenance Services”) during Your license to use the Solution for no charge.

a. Defect Correction. We will use good faith efforts to remediate any defects in the Solution reported by You.

b. Technical Support. You may seek assistance regarding Your use of the Solution by designating up to two (2) of Your employees to coordinate Your requests for Maintenance Services (“Maintenance Services contacts”). Your Maintenance Services contacts may report problems using Our online technical support case management system (https://support.appian.com), by telephone using Our authorized technical support phone line, or using any other means that We may authorize from time-to-time. We shall return support requests within a commercially reasonable time after receipt. Technical support is available 8:00 a.m. to 8:00 p.m. (in the time zone in which the office providing the support is located) Monday through Friday, excluding Our recognized holidays. You shall email support@appian.com with Your Maintenance Services contacts promptly on or after the Effective Date. You may change Your Maintenance Services contacts using Our case management system.

c. Updates. We shall install updates to the Solution as they become available.

d. Your Obligations. You must cooperate with Our reasonable requests in connection with providing the Maintenance Services, including, without limitation, by providing Us with timely access to Your data, information and personnel. You are responsible for the accuracy and completeness of all data and information provided to Us in connection with the Maintenance Services.

e. Excluded Items. Maintenance Services do not include on-site or in-person assistance or consultation, nor extensive training that would normally be provided in formal training classes. In addition, Maintenance Services shall not include technical support or defect correction to the extent required as a result of the following:

i. Use of the Solution contrary to the terms of Our then current documentation associated with the Solution;

ii. Modifications, enhancements or customizations of the Solution;

iii. Any use of the Solution in disregard of any known adverse consequences, including without limitation Your failure to make appropriate backups or to follow warning messages and other written instructions; or

Any other cause not attributable to Us.

**6. Indemnification**

a. Indemnity. Subject to the limitations and contingencies set forth below, We shall at Our expense defend any claim brought against You by a third party alleging that the Solution infringes any patent, copyright, trademark, or other proprietary rights of any third party. As part of Our defense obligations, We will pay all associated and reasonable attorneys’ fees and defense costs, and pay any corresponding judgment finally awarded by a court of competent jurisdiction or any settlement amount agreed to in a written settlement agreement approved by Our duly authorized representative. If the Solution is held by a court of competent jurisdiction to infringe the aforementioned intellectual property rights and Your use of the Solution is enjoined, or We conclude that the Solution infringes the foregoing intellectual property rights of a third party, We may immediately terminate Your license to use the Solution upon written notice.

b. Limitation. Notwithstanding the provisions of subpart 6(a) above, We assume no liability for infringement to the extent arising from: (i) combinations of the Solution with software or hardware not provided by Us, including any of Your software or code, or (ii) modifications to the Solution made by any party other than Us.

c. Contingencies. As a condition to the foregoing indemnity obligations, You shall provide Us with prompt notice of any claim for which indemnification shall be sought hereunder and shall cooperate in all reasonable respects with Us in connection with any such claim. We shall be entitled to control the handling of any such claim and to defend or settle any such claim, in Our sole discretion, with counsel of Our own choosing; provided, however, that We may not agree to any settlement other than the payment of money or release of any claim without Your prior written permission, which shall not be unreasonably withheld, conditioned or delayed. You shall have the right to be represented by advisory counsel at Your expense.

d. Entire Liability. THIS SECTION 6 STATES OUR ENTIRE LIABILITY AND OBLIGATIONS AND YOUR EXCLUSIVE REMEDY WITH RESPECT TO ANY ALLEGED OR ACTUAL INFRINGEMENT OF PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER INTELLECTUAL PROPERTY RIGHTS BY THE SOLUTION OR ANY PART THEREOF.

**7. Termination and Suspension**

a. Termination. Either party may terminate this Agreement in the event of a material breach of this Agreement after thirty days’ notice to the other party and opportunity to cure during the thirty day notice period. In addition, Appian may terminate this Agreement immediately if You are a competitor of Appian, or are providing the Solution or information concerning the Solution to a competitor of Appian.  Upon the termination or expiration of this Agreement, You must cease using the Solution and You must promptly delete all files relating to the Solution. Upon Our written request, You shall confirm that You have complied with the foregoing in writing.

b. Suspension. Upon providing You with written notice, Appian may immediately suspend Your privilege to use the Solution, which suspension shall be without any liability to Appian if Appian has reason to believe: (i) You or Your Users are using the Solution in any manner to (A) interfere or attempt to interfere with the functionality or proper working of the Service, including but not limited to participating in any flooding or denial or service activities of any kind, or (B) engage in, promote or facilitate illegal activities; or (ii) the Data (A) infringes, violates or misappropriates any rights of Appian or any third party; (B) constitutes defamation, invasion of privacy or publicity, or otherwise violates any applicable law or regulation, or (C) contains malware, viruses, Trojan horses, spyware, worms, or other malicious or harmful code.

**8. General Provisions**

a. Waiver. Any waiver by either party of any violation of this Agreement shall not constitute a waiver by such party of any other or future violation of the same provision, or any other provision, of this Agreement.

b. Export. The Solution uses software and technology that may be subject to United States export controls administered by the U.S. Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, and other U.S. agencies and the export control regulations of the European Union and Canada. You acknowledge and agree that the Solution shall not be used, and none of the underlying information, software, or technology may be transferred or otherwise exported or re-exported to countries as to which the United States, Canada and/or the European Union maintains an embargo (collectively, “Embargoed Countries”), or to or by a national or resident thereof, or any person or entity on the U.S. Department of Treasury’s List of Specially Designated Nationals or the U.S. Department of Commerce’s Table of Denial Orders (collectively, “Designated Nationals”). The lists of Embargoed Countries and Designated Nationals are subject to change without notice. By using the Solution, You represent and warrant that You are not located in, under the control of, or a national or resident of an Embargoed Country or Designated National. You agree to comply strictly with all applicable export laws and assume sole responsibility for obtaining any necessary licenses to export or re-export.

c. Notices. All communications and notices to be made or given pursuant to this Agreement shall be in the English language.

i. To You. Except as otherwise set forth herein, notices made by Us to You under this Agreement will be provided to You via the email address provided to Us during Your ordering of the Solution or in any updated email address You provide to Us in accordance with standard account information update procedures We may provide from time-to-time. You must keep Your email address current and You will be deemed to have received any email sent to any such email address, upon Our sending the email, whether or not You actually receive the email.

ii. To Us. Formal legal notices (e.g. notice of breach, etc.) should be sent to the following address or to any updated address that we may notify You of from time-to-time: Appian Corporation, Attention General Counsel, 7950 Jones Branch Drive, Tysons, Virginia (USA) 22102

d. Governing Law.

i. North, Central and South America. If You are located in North, Central of South America (including the Caribbean), this Agreement shall be governed by the laws of the Commonwealth of Virginia (USA) and controlling United States federal law, without regard to the choice or conflicts of law provisions of any jurisdiction, and any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by arbitration in the County of Fairfax, Virginia in accordance with the Rules of the American Arbitration Association (“AAA”). The arbitration shall be conducted by a single arbitrator to be designated by AAA in the English language, and judgment upon the decision rendered by the arbitrator may be entered in any court having jurisdiction thereof. In the event applicable law expressly prohibits the use of the Uniform Computer Information Transactions Act and thereby prohibits the application of Virginia law, then this Agreement shall be governed by the law of the State of Washington (USA) and controlling United States federal law, without regard to the choice or conflicts of law provisions of any jurisdiction, and any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by arbitration in King County, Washington (USA) in accordance with the arbitration rules of the AAA.

ii. Europe, the Middle East or Africa. If You are located in Europe, the Middle East or Africa, this Agreement shall be governed by the laws of England and Wales, without regard to the choice or conflicts of law provisions of any jurisdiction, and any controversy or claim arising from or out of this Agreement, or the breach or interpretation thereof, shall be determined by arbitration in London, England, as administered by the International Centre for Dispute Resolution (“ICDR”) in accordance with its International Arbitration Rules. The arbitration shall be conducted by a single arbitrator designated by the ICDR, and judgment upon the decision rendered by the arbitrator may be entered in any court having jurisdiction thereof.

iii. Asia, Australia, New Zealand and the Pacific Islands. If You are located in Asia, Australia, New Zealand or the Pacific Islands, this Agreement shall be governed by the laws of the Republic of Singapore, without regard to the choice or conflicts of law provisions of any jurisdiction, and any controversy or claim arising from or out of this Agreement, or the breach or interpretation thereof, shall be determined by arbitration in the Republic of Singapore, as administered by the ICDR in accordance with its International Arbitration Rules. The arbitration shall be conducted by a single arbitrator designated by the ICDR, and judgment upon the decision rendered by the arbitrator may be entered in any court having jurisdiction thereof.

iv. General. Notwithstanding what law governs this Agreement, the parties expressly exclude the application of the United Nations Convention for the International Sale of Goods to this Agreement. In addition, notwithstanding what arbitration forum is used to resolve any dispute, (I) the prevailing party in the arbitration proceedings shall be entitled to recover attorney’s fees, and all reasonable out of pocket costs and disbursements, including the cost of the arbitrator, (II) any decision by the arbitrator shall be final and binding, and except in cases of fraud or gross misconduct by the arbitrator, the decision rendered by the arbitrator shall not be appealable, and (III) nothing in this Agreement will prevent either party from seeking injunctive relief to enforce the terms of this Agreement in any competent venue or jurisdiction. Any arbitration proceedings shall be conducted in the English language.

e. Entire Agreement. This Agreement constitutes the entire agreement concerning the subject matter hereof and replaces all prior and concurrent oral or written communications between the parties relating to the subject matter hereof.

f. Amendment. This Agreement may be amended or modified only in a written document signed by authorized representatives of You and Us.

g. Severability. If any provision of this Agreement is found unenforceable, it and any related provisions will be interpreted to best accomplish the unenforceable provision’s essential purpose.

h. Assignment. Neither party shall assign any of its rights nor delegate any of its obligations under this Agreement, by operation of law or otherwise, to any third party without the express prior written consent of the other, non-assigning party. This Agreement shall be binding and inure to the benefit of the parties hereto and their respective and permitted successors and assigns.

i. Headings. The headings used in this Agreement are for convenience of reference only and do not constitute a part of this Agreement. They will not be deemed to limit, characterize or in any way affect any provision of this Agreement, and all provisions of this Agreement will be enforced and construed as if no heading had been used.

j. Survival. All provisions that by their terms or nature survive termination of this Agreement shall survive such termination.

**Schedule 1 -Privacy Obligations.**

We shall process Your Confidential Information and Personal Data (as defined below) only in accordance with Your instructions pursuant to this Schedule 1 and the Agreement.

**1. Definitions**

a. “Data Security Breach” means an unauthorized disclosure of, access to, or acquisition, processing, transfer or disposal of, Your Confidential Information or Personal Data in Our possession through a security breach, loss or corruption or any other circumstances not caused by You or Your agents.

b. “GDPR” means the EU General Data Protection Regulation, adopted in April 2016, which will supersede the EU Data Protection Directive, and is enforceable as of May 25, 2018.

c. “Personal Data” is as defined by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (the “EU Data Protection Directive”) and as defined by GDPR).

d. “Privacy Shield” means the European Union-United States Privacy Shield Framework and/or the Switzerland-US Privacy Shield Framework established by the US Department of Commerce and the European Commission and Switzerland, respectively.

e. “Privacy Shield Principles” means the Privacy Shield principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, Recourse Enforcement and Liability and all applicable Supplemental Principles as set forth by the U.S. Department of Commerce.

f. “Processing” means any operation or set of operations which is performed upon the Your Confidential Information or Personal Data, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, disposal or destruction.

**2. Personal Information Processing**-In the event We have access to or processes Personal Data, We shall comply with all applicable privacy and data protection laws.

a. Data Transfer Agreements. If We receive Personal Data that is subject to the data transfer restrictions of the EU Data Protection Directive or any similar or successor legislation or regulation, We shall, and shall ensure any third-party service provider to Us to, enter into appropriate data transfer agreements as needed to satisfy cross-border transfer obligations relating to Personal Data.

b. Privacy Shield Obligations. We shall comply with the U.S. Department of Commerce Privacy Shield Principles from the Privacy Shield Frameworks and any successor thereto, as may be amended from time-to-time. We shall take all reasonably appropriate legal, organizational and technical measures to protect and safeguard Personal Data, keeping in mind the nature of such data. We agree to: (i) process Personal Data only for limited and specified purposes of performing this Agreement, subject to Your written instructions, (ii) if We self-certify, maintain an active and valid Privacy Shield certification, (iii) process the Personal Data in compliance with both that certification (if applicable) and the Privacy Shield Principles; (iv) notify You if We can no longer process the Personal Information in compliance with both Our Privacy Shield certification (if applicable) and the Privacy Shield Principles, and, in such a case, immediately cease processing or take reasonable and appropriate steps to stop and remediate unauthorized processing.

c. GDPR. We agree, covenant, and warrant that at any and all times during which We processes Personal Data in performing this Agreement that originated from the European Economic Area (collectively, “EEA Personal Data”), We shall: (i) process EEA Personal Data only for the limited and specified purposes set forth in this Agreement; (ii) provide at least the same level of protection for EEA Personal Data received pursuant to this Agreement as is required by the Privacy Shield Principles and the GDPR; (iii) provide You with all reasonable access and assistance that You may require for the purposes of performing audits or inspections of Our conformance to the terms of this Agreement; (iv) notify You if We decide or determine that We can no longer meet Our obligation to provide the same level of protection as is required by the GDPR; (v) upon providing notice under (iv) above, We shall stop Processing all EEA Personal Data, remediate any unauthorized Processing of EEA Personal Data, and take any other reasonable remediation measures requested by You; (vi) notify You of any data subjects’ requests to exercise their rights under applicable data protection laws and regulations, including without limitation rights of access, correction, amendment, blocking and deletion; (vii) assist You as reasonably necessary with responding to such data subjects’ requests; and (viii) make available to You all information necessary to demonstrate its compliance with all of the above obligations.

**3. Notification**– As soon as circumstances make it commercially practicable, We shall notify You:

a. Of any Data Security Breach, including all relevant facts with respect to the Data Security Breach to the extent known. We shall reasonably assist and cooperate with You with any necessary or appropriate disclosures and other investigative, remedial and monitoring measures as a result of any Data Security Breach;

b. Of any request for access to, or information about, any Personal Data or Your Confidential Information from any government official (including any data protection agency or law enforcement agency) (to the extent not prohibited by applicable law);

c. Of any and all requests, complaints or other communications regarding the individual’s Personal Data received from any such individual whose Personal Data is or may be included among the Personal Data supplied by You (unless prohibited by applicable law). We understand that We are not authorized to respond to these requests, unless explicitly authorized by You, except for a request received from a governmental agency with a subpoena or similar legal document compelling disclosure by Us, provided that We notify You in advance of any such disclosure, where possible.

**4. Physical and Environmental Security**

a. Data Processing Facilities. We shall use reasonable efforts to protect the data processing facilities and physical work environment where Personal Data and Your Confidential Information is stored or processed by or on behalf of Us which includes physical entry controls to reasonably ensure that only authorized individuals gain access to such facilities.

b. Access Privileges. We shall use reasonable efforts to only provide access to the data processing facilities and physical work environment where Personal Data and Your Confidential Information are stored or processed by or on behalf of Us to those employees and third parties who have a legitimate business need for such access privileges. When an employee or third party no longer has such a business need for the access privileges assigned to him/her, the access privileges shall be promptly revoked, even if the employee or a third party continues to be an employee of or have a third party relationship with Us.

**5. Human Resources**

a. Background Screens. We shall establish and maintain controls designed to ensure that employees and other third parties who require unencrypted access to the Personal Data and Your Confidential Information are suitably screened. We shall, to the extent permitted by applicable law, conduct criminal background checks as part of pre-employment screening practices for employees. We will not permit an employee or other third parties to have access to Personal Data or Your Confidential Information or perform material aspects of the Agreement if such employee or third parties have failed to pass such background check.

b. Training. We shall provide an appropriate level of supervision, guidance, and training on information security program safeguards and the importance of personal information security to Our employees and any other third parties who require unencrypted access to Personal Data or Your Confidential Information before such access is granted and subsequently on an annual basis.

**6. Destruction**

a. General. We shall take all reasonable steps to securely destroy, or arrange for the secure destruction and permanently erase from all Our hardware and software containing Personal Data and Your Confidential Information received from or through You at the termination of this Agreement, when You request the same and when there is no longer any legitimate business need to retain such information. Upon Your written request, We shall confirm such destruction, in writing. Notwithstanding the above, copies that exist on back up media as a result of Our regularly scheduled network backups need not be returned or destroyed if is realistically unfeasible to do so. In such event, We will extend the protections of this Schedule to such Personal Data and Your Confidential Information until it is destroyed in the natural course of back-ups.

b. Erasure and Re-Use. We shall use reasonable efforts to ensure that storage media used to store or process Personal Data or Your Confidential Information is appropriately wiped or degaussed prior to media reuse and prior to transfer of such media offsite for maintenance or destruction.

**7. Miscellaneous**. If We fail to comply with this Schedule, You may suspend Our right to process the Personal Data and Your Confidential Information, in addition to all other rights and remedies available to You under the Agreement.

**Schedule 2** –**Business Associate Addendum**.

We shall comply with this Schedule to the extent You provide Us with Personal Health Information, as described below, in the course of performing the Agreement. For the purposes of this Schedule, We are referred to as the Business Associate and You are referred to as the Covered Entity.

HIPAA refers to, collectively, the Health Insurance Portability and Accountability Act and its implementing regulations (45 C.F.R. Parts 160-164), and the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009, and its implementing regulations, each as issued and amended by the Secretary.

Capitalized terms used in this Schedule and not otherwise defined herein shall have the meanings set forth in HIPAA, which definitions are hereby incorporated by reference.

**1. Obligations and Activities of Business Associate.**

(a)       Business Associate agrees to use or disclose Protected Health Information only as permitted or required by this Agreement or as Required by Law.

(b)       Business Associate agrees to use reasonable and appropriate safeguards and security measures to prevent Use or Disclosure of Protected Health Information other than as provided for by this Agreement.  Business Associate agrees to implement reasonable and appropriate administrative, technical, and physical measures to protect the confidentiality, integrity, and availability of Electronic Protected Health Information as required by HIPAA.

(c)       Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(d)       Business Associate agrees to report any Use or Disclosure of Protected Health Information not provided for by this Agreement of which Business Associate becomes aware including any Breach of unsecured Protected Health Information, and any successful Security Incident of which it becomes aware.  Business Associate agrees to make the written report to Covered Entity without unreasonable delay but in no event later than ten (10) business days after Business Associate learns of such unauthorized Use or Disclosure, Breach, or Security Incident.  Business Associate agrees to cooperate with Covered Entity in investigating the Breach and in meeting the Covered Entity’s obligations under HIPAA and any other applicable security breach notification laws.  To avoid unnecessary burden on either party, Business Associate shall only be required to report, upon the Covered Entity’s request, successful Security Incidents which Business Associate becomes aware; provided that the Covered Entity’s request shall be made no more often than is reasonable based upon the relevant facts, circumstances and industry standards.

(e)       Business Associate agrees to enter into a written agreement with each Subcontractor (including, without limitation, a Subcontractor that is an agent under applicable law) that creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate, which agreement shall both meet the requirements of 45 C.F.R. §§ 164.504(e) and 164.314(a)(2) and obligate the Subcontractor to comply with restrictions and conditions that are at least as restrictive as the restrictions and conditions that apply to Business Associate under this Agreement, all to the extent required by HIPAA.  Notwithstanding the foregoing, Covered Entity acknowledges that Business Associate is not required to execute Business Associate Agreements prior to disclosing Protected Health Information to (a) employees of its wholly owned subsidiaries, and (b) individuals who are part of Business Associate’s workforce but are on staff as independent contractors.  Business Associate agrees to remain responsible for any breach of this Agreement by such independent contractors or employees of wholly owned subsidiaries as if the independent contractors and/or employees of wholly owned subsidiaries were employees of Business Associate.

(f)        Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the Use and Disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary, in a time and manner as reasonably requested by or designated by the Secretary, for purposes of the Secretary determining Covered Entity’s compliance with the Privacy Rule.

(g)       Business Associate agrees to document such Disclosures of Protected Health Information and information related to such Disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of Disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.  Within ten (10) business days’ notice by Covered Entity to Business Associate that Covered Entity has received a request for an accounting of Disclosures of Protected Health Information (other than Disclosures to which an exception to the accounting requirement applies), Business Associate agrees to make such documentation available to Covered Entity as necessary for Covered Entity to make the accounting required by 45 C.F.R. § 164.528.

(h)       Business Associate agrees to provide access to Protected Health Information about an Individual at the request of Covered Entity, and in the time and manner as reasonably requested by Covered Entity, but no later than ten (10) business days, to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet the requirements under 45 C.F.R. § 164.524.  If Business Associate receives a request for access to Protected Health Information directly from an Individual, Business Associate agrees to forward such request to Covered Entity within five (5) business days.

(i)        Business Associate agrees to make any amendment(s) to Protected Health Information that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Covered Entity, and in the time and manner mutually agreed by the parties.  If Business Associate receives a request for amendment to Protected Health Information directly from an Individual, Business Associate agrees to forward such request to Covered Entity within five (5) business days.

(j)        To the extent reasonable and/or required by applicable law, Business Associate agrees to comply with the determination of a request for restriction to the Use or Disclosure of Protected Health Information and/or determination of a request for alternative methods of confidential communication pursuant to 45 C.F.R § 164.522 at the request of Covered Entity, and in the time and manner mutually agreed to by the parties acting reasonably and in good faith.  If Business Associate receives a request for restriction to the Use or Disclosure of Protected Health Information and/or request for alternative methods of confidential communication directly from an Individual, Business Associate agrees to forward such request to Covered Entity within five (5) business days.

**2. Permitted Uses and Disclosures by Business Associate.** Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in Section 2(a) of this Schedule, provided that such Use or Disclosure would not violate the minimum necessary and/or Limited Data Set requirements of HIPAA.

(a)       Business Associate is permitted to Use or Disclose Protected Health Information to perform the Agreement for, or on behalf of the Covered Entity in Business Associate’s capacity as a Business Associate.  If feasible, Business Associate shall return or destroy all Protected Health Information when such information is no longer required to accomplish such functions, activities, or services in a time and manner mutually agreed to by the parties, but no later than thirty (30) business days of completion of such functions, activities, or services. Business Associate shall be responsible for all costs and expenses related to the return or destruction of such Protected Health Information.

(b)       Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for Business Associate’s proper management, administration and legal responsibilities, provided that Disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it shall remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c)       Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

(d)       Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

**3. Obligations of Covered Entity.** Covered Entity is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Therefore, without limitation:

(a)       Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity  in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate’s Use or Disclosure of Protected Health Information.

(b)       Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate’s Use or Disclosure of Protected Health Information.

(c)       Covered Entity shall notify Business Associate of any restriction to the Use or Disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate’s Use or Disclosure of Protected Health Information.

(d)       Covered entity shall not include Protected Health Information in: (1) information Covered Entity submits to Business Associate’s support personnel through a technical support request or to Business Associate’s community Business Associate’s support forums; and (2) Covered Entity’s address book or directory information.  Further, Covered Entity may not disclose Protected Health Information to Business Associate by electronic mail, voicemail, text, or facsimile.

(e)       Covered Entity is responsible for implementing appropriate privacy and security safeguards in order to protect the Covered Entity’s PHI In compliance with HIPAA and this Agreement. Without limitation, Covered Entity will use the highest level of audit logging In connection with the Covered Entity’s use of Business Associate’s cloud platform (“Cloud Offering”), and maintain the maximum retention of logs In connection with the Covered Entity’s use of the Cloud Offering.

(f)        Business Associate is responsible for enabling the Cloud Offering to support encryption of PHI in the Cloud Offering.  The Covered Entity is solely responsible for configuring, and will configure, appropriate privacy and security safeguards in all instances of the Cloud Offering that Covered Entity controls, uses, configures and uploads into the Cloud Offering as follows:

The Covered Entity must encrypt all PHI stored in or transmitted using the Cloud Offering in accordance with the Secretary of HHS’s Guidance to Render Unsecured Protected Health information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html> as it may be updated from time to time, and as may be made available on any successor or related site designated by HHS.

**4. Permissible Requests by Covered Entity.** Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, unless otherwise noted in this Agreement.

**5. Term and Termination.**

(a)        **Term.** Notwithstanding anything else in the Agreement to the contrary, the provisions of this Schedule shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b)        **Termination for Cause.** Upon Covered Entity’s knowledge of a material breach of this Schedule by Business Associate, Covered Entity shall either:

(i)        Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(ii)       Immediately terminate the Agreement if Business Associate has breached a material term of this Schedule and cure is not possible; or

(iii)      If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(c)        **Effect of Termination.**

(i)        Except as provided in paragraph (ii) below of this section, upon termination of the Agreement, for any reason, Business Associate shall, if feasible, return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity in the time and manner mutually agreed to by the parties, acting reasonably and in good faith.  This provision shall also apply to Protected Health Information that is in the possession of Subcontractors or agents of Business Associate.  If feasible, Business Associate, Subcontractors, or agents of Business Associate shall retain no copies of the Protected Health Information. Business Associate shall be responsible for all costs and expenses related to the return or destruction of such Protected Health Information.

(ii)       In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible.  Business Associate shall extend the protections of this Schedule to such Protected Health Information and limit further Uses and Disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

(d)        **Cure of Breach.** Covered Entity shall provide an opportunity for Business Associate to cure a breach within the time specified by Covered Entity, which in no event shall be less than thirty (30) calendar days.

**6. Miscellaneous.**

(a)        **Regulatory References.** A reference in this Agreement to HIPAA includes the implementing regulations as issued and amended by the Secretary.

(b)        **Amendment.**

(i)       The parties acknowledge and agree that the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) and its implementing regulations impose requirements with respect to privacy, security and breach notification applicable to Business Associates (collectively, the “**HITECH BA Provisions**”).  The HITECH BA Provisions, any future amendments to or additional regulations issued under the HITECH Act or any other provision of HIPAA that affects Business Associate agreements are hereby incorporated by reference into this Schedule as if set forth in this Schedule in their entirety, effective on the later of the Effective Date or such subsequent effective date as may be specified by HIPAA.

(c)      **Survival.** The respective rights and obligations of Business Associate and Covered Entity under Section 5(c) and Section 1(l) of this Schedule shall survive the termination of the Agreement.