DATA USE AGREEMENT BETWEEN THE
SOUTH ALAMO REGIONAL ALLIANCE FOR THE HOMELESS
AND USER

This Data Use Agreement ("DUA"), effective as of (mm/dd/yyyy) _____, ("Effective Date"), is entered into by and between the **South Alamo Regional Alliance for the Homeless ("SARAH")** and (name of entity) _____, a _____("**User**"), each referred to individually as "**Party**", and collectively as the "**Parties**."

WHEREAS, SARAH, the CoC Lead Agency in San Antonio/ Bexar County and a 501(c)(3) nonprofit, aims to prevent and end homelessness in San Antonio/Bexar County and for homelessness to be a rare, brief, or a nonrecurring event;

WHEREAS, SARAH, the CoC Lead Agency in San Antonio/ Bexar County, is a 501 (c) (3) nonprofit and is a partner with Haven for Hope (Haven), which is a Business Associate (as defined in 45 CFR Part 160-164) of the City of San Antonio and the Bexar County Board of Trustees for Mental Health Mental Retardation Services d/b/a "The Center for Health Care Services", and is also subject to a Data Use Agreement with the Texas Health and Human Services Enterprise Agency Department of State Health Services (collectively "**Third Parties**"); and is therefore subject to HIPAA (the Health Insurance Portability and Accountability Act of 1996);

WHEREAS, the User needs the data to conduct studies and/or outreach on methods and tools for understanding homelessness trends and causes, and for such purpose, has requested access to certain information from SARAH that constitutes Confidential Information as defined herein below; and

WHEREAS, as a pre-condition of allowing the User access to any Confidential Information (but without any obligation to make such information available), the Parties are entering into this Agreement in order to protect and ensure the use of Confidential Information for the studies or outreach endeavors explained in their data request.

NOW THEREFORE, in consideration of the premises and other good and valuable consideration, receipt and sufficiency of which is acknowledged, and intending to be legally bound hereby, the Parties agree as follows:

ARTICLE 1. PURPOSE; APPLICABILITY; ORDER OF PRECEDENCE

The purpose of this DUA is to facilitate access to, creation, receipt, maintenance, use, disclosure or transmission of Confidential Information with User, and describe User's rights and obligations with respect to the Confidential Information and the limited purposes for which the User may create, receive, maintain, use, disclose or have access to Confidential Information. This DUA also describes SARAH's remedies in the event of User's noncompliance with its

obligations under this DUA. This DUA applies to both SARAH business associates, as "business associate" is defined in the Health Insurance Portability and Accountability Act (HIPAA), and Users who are not business associates, who create, receive, maintain, use, disclose or have access to Confidential Information on behalf of SARAH, its programs or clients. As a best practice, SARAH requires its Users to comply with the terms of this DUA to safeguard all types of Confidential Information.

As of the Effective Date of this DUA, if any provision of any other contract or agreement conflicts with this DUA, this DUA controls.

ARTICLE 2.
DEFINITIONS

For the purposes of this DUA, capitalized, underlined terms have the following meanings:

"Authorized Purpose" means the specific purpose or purposes described in the written data request. The User will fulfill its obligations under the data request, or any other purpose expressly authorized by SARAH.

"Authorized User" means a person:

(1) Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this DUA;

(2) For whom User warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and

(3) Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this DUA.

"Breach" means an impermissible use or disclosure of electronic or non-electronic sensitive personal information by an unauthorized person or for an unauthorized purpose that compromises the security or privacy of Confidential Information such as that the use or disclosure poses a risk of reputational harm, theft of financial information, identity theft, or medical identity theft. Any acquisition, access, use, disclosure or loss of Confidential Information other than as permitted by this DUA shall be presumed to be a Breach unless User demonstrates, based on a risk assessment, that there is a low probability that the Confidential Information has been compromised.

"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to User or that User may create, receive, maintain, use, disclose or have access to as part of this agreement with SARAH that consists of or includes any or all of the following:

(1) Education records as defined in the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g; 34 C.F.R. Part 99

(2) Federal Tax Information as defined in Internal Revenue Code §6103 and Internal Revenue Service Publication 1075;

(3) Personal Identifying Information (PII) as defined in Texas Business and Commerce

Code, Chapter 521;

(4) Protected Health Information (PHI) in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information as defined in 45 C.F.R. §160.103;

(5) Sensitive Personal Information (SPI) as defined in Texas Business and Commerce Code, Chapter 521;

(6) Social Security Administration Data, including, without limitation, Medicaid information means disclosures of information made by the Social Security Administration or the Centers for Medicare and Medicaid Services from a federal system of records for administration of federally funded benefit programs under the Social Security Act, 42 U.S.C., Chapter 7;

(7) All privileged work product;

(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

"Destroy", "Destruction", for Confidential Information, means:

(1) Paper, film, or other hard copy media have been shredded or destroyed such that the Confidential Information cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

(2) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization," such that the Confidential Information cannot be retrieved.

"Discover, Discovery" means the first day on which a Breach becomes known to User, or, by exercising reasonable diligence would have been known to User.

"Legally Authorized Representative" of an individual, including as provided in 45 CFR 435.923 (authorized representative); 45 CFR 164.502(g)(1) (personal representative); Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164 (medical power of attorney); and Texas Estates Code § 22.031 (representative).

"Required by Law" means a mandate contained in law that compels an entity to use or disclose Confidential Information that is enforceable in a court of law, including court orders, warrants, subpoenas or investigative demands.

"SubUser" means a person who contracts with a prime User to work, to supply commodities, or to contribute toward completing work for a governmental entity.

"Workforce" means employees, volunteers, trainees or other persons whose performance of work is under the direct control of a party, whether or not they are paid by that party.

ARTICLE 3. USER'S DUTIES REGARDING CONFIDENTIAL INFORMATION

Section 3.01 Obligations of User

User agrees that:

(A) With respect to PHI, User shall:

(1) Make PHI available in a designated record set if requested by SARAH, if User maintains PHI in a designated record set, as defined in HIPAA.

(2) Provide to SARAH data aggregation services related to the healthcare operations User performs for SARAH, if requested by SARAH, if User provides data aggregation services as defined in HIPAA.

(3) Provide access to PHI to an individual who is requesting his or her own PHI, or such individual's Legally Authorized Representative, in compliance with the requirements of HIPAA.

(4) Make PHI available to SARAH for amendment, and incorporate any amendments to PHI that SARAH directs, in compliance with HIPAA.

(5) Document and make available to SARAH, an accounting of disclosures in compliance with the requirements of HIPAA.

(6) If User receives a request for access, amendment or accounting of PHI by any individual, promptly forward the request to SARAH or, if forwarding the request would violate HIPAA, promptly notify SARAH of the request and of User's response. SARAH will respond to all such requests, unless User is Required by Law to respond or SARAH has given prior written consent for User to respond to and account for all such requests.

(B) With respect to ALL Confidential Information, User shall:

(1) Exercise reasonable care and no less than the same degree of care User uses to protect its own confidential, proprietary and trade secret information to prevent Confidential Information from being used in a manner that is not expressly an Authorized Purpose or as Required by Law. User will access, create, maintain, receive, use, disclose, transmit or Destroy Confidential Information in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses.

(2) Establish, implement and maintain appropriate procedural, administrative, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, in accordance with applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as User has such Confidential Information in its actual or constructive possession.

(3) Implement, update as necessary, and document privacy, security and Breach notice policies and procedures and an incident response plan to address a Breach, to comply with the privacy, security and breach notice requirements of this DUA prior to conducting any work.

(4) Obtain SARAH's prior written consent to disclose or allow access to any portion of the Confidential Information to any person, other than Authorized Users, Workforce or SubUsers of User who have completed training in confidentiality, privacy, security and the

importance of promptly reporting any Breach to User's management and as permitted in Section 3.01(A)(3), above.

(5) Establish, implement and maintain appropriate sanctions against any member of its Workforce or SubUser who fails to comply with this DUA or applicable law. User shall maintain evidence of sanctions and produce it to SARAH upon request.

(6) Obtain prior written approval of SARAH, to disclose or provide access to any Confidential Information on the basis that such act is Required by Law, so that SARAH may have the opportunity to object to the disclosure or access and seek appropriate relief. If SARAH objects to such disclosure or access, User shall refrain from disclosing or providing access to the Confidential Information until SARAH has exhausted all alternatives for relief.

(7) Certify that its Authorized Users each have a demonstrated need to know and have access to Confidential Information solely to the minimum extent necessary to accomplish the Authorized Purpose and that each has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in this DUA. User and its SubUsers shall maintain at all times an updated, complete, accurate list of Authorized Users and supply it to SARAH upon request.

(8) Provide, and shall cause its SubUsers and agents to provide, to SARAH periodic written confirmation of compliance with controls and the terms and conditions of this DUA.

(9) Return to SARAH or Destroy, at SARAH's election and at User's expense, all Confidential Information received from SARAH or created or maintained by User or any of User's agents or SubUsers on SARAH's behalf upon the termination or expiration of this DUA, if reasonably feasible and permitted by law. User shall certify in writing to SARAH that all such Confidential Information has been Destroyed or returned to SARAH, and that User and its agents and SubUsers have retained no copies thereof. Notwithstanding the foregoing, User acknowledges and agrees that it may not Destroy any Confidential Information if federal or state law, or SARAH record retention policy or a litigation hold notice prohibits such Destruction. If such return or Destruction is not reasonably feasible, or is impermissible by law, User shall immediately notify SARAH of the reasons such return or Destruction is not feasible and agree to extend the protections of this DUA to the Confidential Information for as long as User maintains such Confidential Information.

(10) Comply with the SARAH Acceptable Use standards which require each SubUser and its employees, contractors, consultants, temporary, and its subsidiaries to be responsible for exercising good judgment regarding appropriate use of information, electronic devices, and establish secure network resources to protect Confidential Information.

(11) Only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form. A secure transmission of electronic Confidential Information *in motion* includes secure File Transfer Protocol (SFTP) or encryption at an appropriate level as required by rule, regulation or law. Confidential Information *at rest* requires encryption unless there is adequate administrative, technical, and physical security as required by rule, regulation or law. All electronic data transfer and communications of Confidential Information shall be through secure systems. User shall provide proof of system, media or device security and/or encryption to SARAH no later

than 48 hours after SARAH's written request in response to a compliance investigation, audit, or the Discovery of a Breach. SARAH may also request production of proof of security at other times as necessary to satisfy state and federal monitoring requirements. Deidentification of Confidential Information in accordance with HIPAA de-identification standards is deemed secure.

(12) Make available to SARAH any information SARAH requires to fulfill SARAH's obligations to provide access to, or copies of, Confidential Information in accordance with applicable laws, regulations or demands of a regulatory authority relating to Confidential Information. User shall provide such information in a time and manner reasonably agreed upon or as designated by the applicable law or regulatory authority.

(13) Comply with the following laws and standards ***if applicable to the type of Confidential Information and User's Authorized Purpose***:

- Title 1, Part 10, Chapter 202, Subchapter B, Texas Administrative Code;
- The Privacy Act of 1974;
- OMB Memorandum 17-12;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Internal Revenue Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies;
- National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1
- An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- NIST Special Publications 800-53 and 800-53A – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems;
- NIST Special Publication 800-88, Guidelines for Media Sanitization;
- NIST Special Publication 800-111, Guide to Storage of Encryption Technologies for End User Devices containing PHI;
- Family Educational Rights and Privacy Act
- Texas Business and Commerce Code, Chapter 521;
- Any other State or Federal law, regulation, or administrative rule relating to the specific SARAH program area that User supports on behalf of SARAH.

(14) Be permitted to use or disclose Confidential Information for the proper management and administration of User or to carry out User's legal responsibilities, except as otherwise limited by this DUA or law applicable to the Confidential Information, if:

(a) Disclosure is Required by Law;

(b) User obtains reasonable assurances from the person to whom the information is disclosed that the person shall:

1. Maintain the confidentiality of the Confidential Information in accordance with this DUA;

2. Use or further disclose the information only as Required by Law or for the Authorized Purpose for which it was disclosed to the person; and

3. Notify User in accordance with Section 4.01 of a Breach of Confidential Information that the person Discovers or should have Discovered with the exercise of reasonable diligence.

(C) With respect to ALL Confidential Information, User shall NOT:

(1) Attempt to re-identify or further identify Confidential Information that has been deidentified or attempt to contact any persons whose records are contained in the Confidential Information, except for an Authorized Purpose, without express written authorization from SARAH.

(2) Engage in prohibited marketing or sale of Confidential Information.

(3) Permit, or enter into any agreement with a SubUser to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information, on behalf of SARAH without requiring that SubUser first execute either the Form SubUser Agreement, Attachment 1, or User's own SubUser agreement that ensures that the SubUser shall comply with the same safeguards and restrictions contained in this DUA for Confidential Information. User is directly responsible for its SubUsers' compliance with, and enforcement of, this DUA.

ARTICLE 4. BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

Section 4.01. Cooperation and Financial Responsibility.

(A) User shall, at User's expense, cooperate fully with SARAH in investigating, mitigating to the extent practicable, and issuing notifications as directed by SARAH, for any Breach of Confidential Information.

(B) User shall make Confidential Information in User's possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach.

(C) User's obligation begins at the Discovery of a Breach and continues as long as related activity continues, until all effects of the Breach are mitigated to SARAH's satisfaction (the "incident response period").

Section 4.02. Initial Breach Notice.

For federal information ***obtained from a federal system of records***, including Federal Tax Information and Social Security Administration Data (which includes Medicaid and other governmental benefit program Confidential Information), User shall notify SARAH of the Breach within the first clock hour in the next business day of Discovery. For all other types of Confidential Information User shall notify SARAH of the Breach not more than 24 hours after Discovery, ***or in a timeframe otherwise approved by SARAH in writing.*** User shall initially report to SARAH's Privacy and Security Officers via email at: data@sarahomeless.org.

User shall report all information reasonably available to User about the Breach.

User shall provide contact information to SARAH for User's single point of contact who will communicate with SARAH both on and off business hours during the incident response period.

Section 4.03 Third Business Day Notice: No later than 5 p.m. on the third business day after Discovery, or a time within which Discovery reasonably should have been made by User of a Breach of Confidential Information, User shall provide written notification to SARAH of all reasonably available information about the Breach, and User's investigation, including, to the extent known to User:

a. The date the Breach occurred;

b. The date of User's and, if applicable, SubUser's Discovery;

c. A brief description of the Breach, including how it occurred and who is responsible (or hypotheses, if not yet determined);

d. A brief description of User's investigation and the status of the investigation;

e. A description of the types and amount of Confidential Information involved;

f. Identification of and number of all individuals reasonably believed to be affected, including first and last name of the individual and if applicable, the Legally authorized representative, last known address, age, telephone number, and email address if it is a preferred contact method;

g. User's initial risk assessment of the Breach demonstrating whether individual or other notices are required by applicable law or this DUA for SARAH approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;

h. User's recommendation for SARAH's approval as to the steps individuals and/or User on behalf of individuals, should take to protect the individuals from potential harm, including User's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an individual with special capacity or circumstances;

i. The steps User has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);

j. The steps User has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Breach;

k. Identify, describe or estimate of the persons, Workforce, SubUser, or individuals and any law enforcement that may be involved in the Breach;

l. A reasonable schedule for User to provide regular updates regarding response to the Breach, but no less than every three (3) business days, or as otherwise directed by SARAH in writing, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and

m. Any reasonably available, pertinent information, documents or reports related to a Breach that SARAH requests following Discovery.

Section 4.04. Investigation, Response and Mitigation.

(A) User shall immediately conduct a full and complete investigation, respond to the Breach, commit necessary and appropriate staff and resources to expeditiously respond, and report as required to SARAH for incident response purposes and for purposes of SARAH's compliance with report and notification requirements, to the satisfaction of SARAH.

(B) User shall complete or participate in a risk assessment as directed by SARAH following a Breach, and provide the final assessment, corrective actions and mitigations to SARAH for review and approval.

(C) User shall fully cooperate with SARAH to respond to inquiries and/or proceedings by state and federal authorities, persons and/or individuals about the Breach.

(D) User shall fully cooperate with SARAH's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such Breach, or to recover or protect any Confidential Information, including complying with reasonable corrective action or measures, as specified by SARAH in a Corrective Action Plan if directed by SARAH.

Section 4.05. Breach Notification to Individuals and Reporting to Authorities.

(A) SARAH may direct User to provide Breach notification to individuals, regulators or third-parties, as specified by SARAH following a Breach.

(B) User must comply with all applicable legal and regulatory requirements in the time, manner and content of any notification to individuals, regulators or third-parties, or any notice required by other state or federal authorities, including without limitation, notifications required by Texas Business and Commerce Code, Chapter 521.053(b) and HIPAA. Notice letters will be in User's name and on User's letterhead, unless otherwise directed by SARAH, and will contain contact information, including the name and title of User's representative, an email address and a toll-free telephone number, for the individual to obtain additional information.

(C) User shall provide SARAH with draft notifications for SARAH approval prior to distribution and copies of distributed and approved communications.

(D) User shall have the burden of demonstrating to the satisfaction of SARAH that any required notification was timely made. If there are delays outside of User's control, User shall provide written documentation to SARAH of the reasons for the delay.

(E) If SARAH directs User to provide notifications, SARAH shall, in the time and manner reasonably requested by User, cooperate and assist with User's information requests in order to make such notifications.

ARTICLE 5. GENERAL PROVISIONS

Section 5.01 Ownership of Confidential Information

User acknowledges and agrees that the Confidential Information is and shall remain the property of SARAH. User agrees it acquires no title or rights to the Confidential Information.

Section 5.02 SARAH Commitment and Obligations

SARAH will not request User to create, maintain, transmit, use or disclose PHI in any manner that would not be permissible under applicable law if done by SARAH.

Section 5.03 SARAH Right to Inspection

At any time upon reasonable notice to User, or if SARAH determines that User has violated this DUA, SARAH, directly or through its agent, will have the right to inspect the facilities, systems, books and records of User to monitor compliance with this DUA. For purposes of this subsection, SARAH's agent(s) include, without limitation, the SARAH Office of the Inspector General, the Office of the Attorney General of Texas, the State Auditor's Office, outside consultants, legal counsel or other designee.

Section 5.04 Term; Termination of DUA; Survival

This DUA will be effective on the date on which User and SARAH have executed the DUA and will terminate as set forth herein.

(A) If SARAH determines that User has violated a material term of this DUA; SARAH may in its sole discretion:

(1) Exercise any of its rights including but not limited to reports, access and inspection under this DUA; or

(2) Require User to submit to a corrective action plan, including a plan for monitoring and plan for reporting as SARAH may determine necessary to maintain compliance with this DUA; or

(3) Provide User with a reasonable period to cure the violation as determined by SARAH; or

(4) Terminate the DUA immediately and seek relief in a court of competent jurisdiction in Bexar County, Texas.

Before exercising any of these options, SARAH will provide written notice to User describing the violation and the action it intends to take.

(B) If neither termination nor cure is feasible, SARAH shall report the violation to the applicable regulatory authorities.

(C) The duties of User or its SubUser under this DUA survive the expiration or termination of this DUA until all the Confidential Information is Destroyed, as required by this DUA.

Section 5.05 Injunctive Relief

(A) User acknowledges and agrees that SARAH may suffer irreparable injury if User or its SubUser fails to comply with any of the terms of this DUA with respect to the Confidential Information or a provision of HIPAA or other laws or regulations applicable to Confidential Information.

(B) User further agrees that monetary damages may be inadequate to compensate SARAH for User's or its SubUser's failure to comply. Accordingly, User agrees that SARAH will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without posting a bond and without the necessity of demonstrating actual damages, to enforce the terms of this DUA.

Section 5.06 Indemnification

User shall indemnify, defend and hold harmless SARAH and its respective Executive Director, employees, SubUsers, agents (including other state agencies acting on behalf of SARAH) or other members of SARAH' Workforce (each of the foregoing hereinafter referred to as "Indemnified Party") against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this DUA or from any acts or omissions related to this DUA by User or its employees, directors, officers, SubUsers, or agents or other members of User's Workforce. The duty to indemnify, defend and hold harmless is independent of the duty to insure. Upon demand, User shall reimburse SARAH for any and all losses, liabilities, lost profits, fines, penalties, costs or expenses (including costs of required notices, investigation, and mitigation of a Breach, fines or penalties imposed on an Indemnified Party by a regulatory authority, and reasonable attorneys' fees) which may be imposed upon any Indemnified Party to the extent caused by and which results from the User's failure to meet any of its obligations under this DUA. User's obligation to defend, indemnify and hold harmless any Indemnified Party will survive the expiration or termination of this DUA.

Section 5.08 Entirety of the Contract

This DUA constitutes the entire agreement between the parties. No change, waiver, or discharge of obligations arising under those documents will be valid unless in writing and executed by the party against whom such change, waiver, or discharge is sought to be enforced.

Section 5.09 Automatic Amendment and Interpretation

Upon the effective date of any amendment or issuance of additional regulations to any law applicable to Confidential Information, this DUA will automatically be amended so that the obligations imposed on SARAH and/or User remain in compliance with such requirements. Any ambiguity in this DUA will be resolved in favor of a meaning that permits SARAH and User to comply with laws applicable to Confidential Information.

Section 5.10 Notices; Requests for Approval

All notices and requests for approval related to this DUA will be evaluated by SARAH's PII Review Team after the User submits a request. All questions relate to this DUA must be directed to the SARAH's Security Officer at data@sarahomeless.org.

WITNESS HEREOF, the Parties have caused their duly authorized representatives to enter into this Agreement as of the Effective Date.

SOUTH ALAMO REGIONAL ALLIANCE FOR THE HOMELESS	**USER: [NAME of ENTITY]**
By: _____	**By**: _____
Title: Executive Director	Title: _____
Date: _____	**Date**: _____

ATTACHMENT 1. SUBUSER AGREEMENT FORM

SARAH CONTRACT NUMBER

_____

The DUA between SARAH and User establishes the permitted and required uses and disclosures of Confidential Information by User.

User has subcontracted with (Name of Entity) _____(SubUser) for performance of duties on behalf of USER which are subject to the DUA. SubUser acknowledges, understands and agrees to be bound by the same terms and conditions applicable to User under the DUA, incorporated by reference in this Agreement, with respect to SARAH Confidential Information. User and SubUser agree that SARAH is a third-party beneficiary to applicable provisions of the subcontract.

SARAH has the right, but not the obligation, to review or approve the terms and conditions of the subcontract by virtue of this SubUser Agreement Form.

User and SubUser assure SARAH that any Breach as defined by the DUA that SubUser Discovers shall be reported to SARAH by User in the time, manner and content required by the DUA.

If User knows or should have known in the exercise of reasonable diligence of a pattern of activity or practice by SubUser that constitutes a material breach or violation of the DUA or the SubUser's obligations, User shall:

1. Take reasonable steps to cure the violation or end the violation, as applicable;
2. If the steps are unsuccessful, terminate the contract or arrangement with SubUser, if feasible;
3. Notify SARAH upon Discovery of the pattern of activity or practice of SubUser that constitutes a material breach or violation of the DUA and keep SARAH reasonably and regularly informed about steps User is taking to cure or end the violation or terminate SubUser's contract or arrangement.

This SubUser Agreement Form is executed by the parties in their capacities indicated below.

USER	**SUBUSER**
Organization: _____	**Organization**_____
NAME: _____	**NAME:**_____
TITLE: _____	**TITLE:**_____
DATE _____	**DATE**_____

This Page is Intentionally Left Blank