

## DATA USE AGREEMENT

### BETWEEN CoC LEAD, HMIS LEAD, AND USER

This Data Use Agreement (“DUA” or “Agreement”), effective as of (“Effective Date”), is entered into by and between the South Alamo Regional Alliance for the Homeless d/b/a Close to Home (“Close to Home” or “CoC Lead”), Haven for Hope of Bexar County (“Haven” or “HMIS Lead”), and (“User”), each referred to individually as “Party”, and collectively as the “Parties”.

WHEREAS, Close to Home, 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, Close to Home serves as the governing body that selects the HMIS Lead Agency for the City of San Antonio and the Bexar County Continuum of Care (“CoC”) and has selected Haven for Hope of Bexar County (“Haven” or “HMIS Lead”) as the HMIS Lead Agency, which manages the operations of the Homeless Management Information System (“HMIS”) on behalf of the CoC Board and provides HMIS administration functions, including Data Privacy and Security, at the direction of the CoC Board;

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

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

The purpose of this DUA is to facilitate access to, creation, receipt, maintenance, use, disclosure or transmission of Confidential Information by 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, transmit, or have access to Confidential Information. This DUA also describes the Parties’ remedies in the event of User’s noncompliance with its obligations under this DUA. This DUA applies to both CoC Lead and HMIS Lead 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 the CoC Lead or HMIS Lead, its programs or clients. As a best practice, CoC Lead and HMIS Lead require its Users to comply with the terms of this DUA to safeguard all types of Confidential Information.

#### ARTICLE 2. DEFINITIONS

For the purposes of this DUA, **capitalized or underlined terms that are not otherwise defined in this Agreement have the meanings set forth in the following (as amended or replaced from time to time):** Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (42 U.S.C. §1320d, *et seq.*)

and regulations thereunder in 45 CFR Parts 160 and 164, including all amendments, regulations and guidance issued thereafter; 42 CFR Part 2; the HMIS Privacy and Security Standards published by the U.S. Department of Housing and Urban Development on July 30, 2004 at Federal Register, Vol. 69; The Social Security Act, including Section 1137 (42 U.S.C. §§ 1320b-7), Title XVI of the Act; The Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a and regulations and guidance thereunder; Internal Revenue Code, Title 26 of the United States Code and regulations and publications adopted under that code, including IRS Publication 1075; OMB Memorandum 07-18; the Texas Health and Safety Code Ch. 181; the Texas Business and Commerce Code Ch. 521; Texas Government Code, Ch. 552, and Texas Government Code §2054.1125. In addition, the following terms in this DUA are defined as follows:

“**Authorized Purpose**” means the use of Confidential Information by User solely for the purpose of the Data Request, attached hereto as **Exhibit A**.

“**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 for the Authorized Purpose 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 for the Authorized Purpose; 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. Breach includes the acquisition, access, use, or disclosure of Protected Health Information in a manner that compromises the security or privacy of the Protected Health Information. 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.

“**Client Information**” means any and all non-public, personally identifiable information and non-personally identifiable information concerning any individual receiving homelessness services from Haven or other service providers in San Antonio/Bexar County, which is inputted into HMIS and is or may be disclosed to User under this DUA.

“**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, transmit, or have access to under or in connection with this Agreement, that consists of or includes any or all of the following:

- (1) Client Information;
- (2) 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; Sensitive Personal Information defined by Texas Business and Commerce Code Chapter 521;

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

(4) Personally Identifiable Information (PII) as defined by Texas Business and Commerce Code, Chapter 521;

(5) Social Security Administration Data, including, without limitation, Medicaid/Medicare information and 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;

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

(7) All privileged work product;

(8) All information and data stored in the Homeless Management Information System (HMIS); and

(9) 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”** or **“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”** or **“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 the 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); 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.

**“Subcontractor”** means a person who contracts with User to work, to supply commodities, or to contribute toward completing work under this DUA.

**“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 said Party.

## ARTICLE 3. USER'S DUTIES REGARDING CONFIDENTIAL INFORMATION

### **Section 3.01.    *Obligations of User***

User agrees that:

(A) User will not provide or otherwise disclose Confidential Information in any form to any person or entity and will use Confidential Information solely for the Authorized Purpose. Any reports, compilations, databases, systems, software programs, analyses, summaries, and other forms of information that are prepared by User with information obtained from CoC Lead or HMIS Lead and disclosed to any other persons or entities, including to other departments within User, shall contain only de-identified information in aggregate form (as defined under the HIPAA regulations) and shall not identify any particular individual(s). Failure to comply with this subsection is deemed to be a material breach of this Agreement. Under no circumstances will User disclose or allow Confidential Information to be used, for law enforcement or prosecution purposes, including, without limitation, to locate suspects or witnesses, to serve warrants, or as evidence in any proceeding.

(B) User will 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 any portion of the Confidential Information from being used in a manner that is not expressly an Authorized Purpose under this DUA or as Required by Law. **45 CFR 164.502(b); 45 CFR 164.514(d)**

(C) User will not, without the CoC Lead and HMIS Lead prior written consent, disclose or allow access to any portion of the Confidential Information to any Person or other entity, other than Authorized User's Workforce or Subcontractors of User who have completed training in confidentiality, privacy, security and the importance of promptly reporting any Event or Breach to User's management, to carry out the Authorized Purpose or as Required by Law.

User will produce evidence of completed training to CoC Lead and HMIS Lead upon request. **45 C.F.R. 164.308(a)(5)(i); Texas Health & Safety Code §181.101**

(D) User will establish, implement and maintain appropriate sanctions against any member of its Workforce or Subcontractor who fails to comply with this DUA or applicable law. User will maintain evidence of sanctions and produce it to CoC Lead and HMIS Lead upon request. **45 C.F.R. 164.308(a)(1)(ii)(C); 164.530(e); 164.410(b); 164.530(b)(1)**

(E) User will not, without prior written approval of CoC Lead and HMIS Lead, disclose or provide access to any Confidential Information on the basis that such act is Required by Law without notifying CoC Lead and HMIS Lead so that CoC Lead and HMIS Lead may have the opportunity to object to the disclosure or access and seek appropriate relief. If Coc Lead and HMIS Lead objects to such disclosure or access, User will refrain from disclosing or providing access to the Confidential Information until CoC Lead and HMIS Lead have exhausted all alternatives for relief. **45 CFR 164.504(e)(2)(ii)(A)**

(F) User will not attempt to re-identify or further identify Confidential Information or De-identified Information, or attempt to contact any Individuals whose records are contained in the Confidential Information, without express written authorization from CoC Lead and HMIS Lead. **45 CFR 164.502(d)(2)(i) and (ii)** User will not engage in prohibited marketing or sale of Confidential Information. **45 CFR 164.501, 164.508(a)(3) and (4); Texas Health & Safety Code Ch. 181.002**

(G) User will not permit, or enter into any agreement with a Subcontractor to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information, on behalf of User without requiring that Subcontractor first execute a written agreement that ensures the Subcontractor will comply with the identical terms, conditions, safeguards and restrictions as contained in this DUA; and **45 CFR 164.502(e)(1)(ii); 164.504(e)(1)(i) and (2)**

**(H)** User is directly responsible for compliance with, and enforcement of, all conditions for creation, maintenance, use, disclosure, transmission and Destruction of Confidential Information and the acts or omissions of Subcontractors as may be reasonably necessary to prevent unauthorized use. **45 CFR 164.504(e)(5); 42 CFR 431.300, et seq.**

**(I)** If User maintains PHI in a Designated Record Set, User will make PHI available to CoC Lead and HMIS Lead on request in a Designated Record Set or, as directed by CoC Lead and HMIS Lead, provide PHI to the Individual, or Legally Authorized Representative of the Individual who is requesting PHI in compliance with the requirements of the HIPAA Privacy Regulations. User will make other Confidential Information in User's possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach of Unsecured PHI by User, (including any of its Workforce or Subcontractors) as defined in HIPAA. **45 CFR 164.524 and 164.504(e)(2)(ii)(E)**

**(J)** User will make PHI as required by HIPAA available to CoC Lead and HMIS Lead for amendment and incorporate any amendments to this information that CoC Lead and HMIS Lead directs or agrees to pursuant to the HIPAA. **45 CFR 164.504(e)(2)(ii)(E) and (F)**

**(K)** User will document and make available to CoC Lead and HMIS Lead the PHI required to provide access, an accounting of disclosures or amendment in compliance with the requirements of the HIPAA Privacy Regulations. **45 CFR 164.504(e)(2)(ii)(G) and 164.528**

**(L)** If User receives a request for access, amendment or accounting of PHI by any Individual subject to this DUA, it will promptly forward the request to CoC Lead and HMIS Lead; however, if it would violate HIPAA to forward the request, User will promptly notify CoC Lead and HMIS Lead of the request and of User's response. Unless User is prohibited by law from forwarding a request, CoC Lead and HMIS Lead will respond to all such requests, unless CoC Lead and HMIS Lead has given prior written consent for User to respond to and account for all such requests. **45 CFR 164.504(e)(2)**

**(M)** User will provide, and will cause its Subcontractors and agents to provide, to CoC Lead and HMIS Lead periodic written certifications of compliance with controls and provisions relating to information privacy, security and breach notification, including without limitation information related to data transfers and the handling and disposal of Confidential Information. **45 CFR 164.308; 164.530(c); 1 TAC 202**

**(N)** Except as otherwise limited by this DUA or law applicable to the Confidential Information, User may use or disclose PHI for the proper management and administration of User or to carry out User's legal responsibilities if: **45 CFR 164.504(e)(4)(ii)**

- (1) Disclosure is Required by Law, provided that User complies with Section 3.01(D);
- (2) User obtains reasonable assurances from the Person to whom the information is disclosed that the Person will:
  - (a) Maintain the confidentiality of the Confidential Information in accordance with this DUA;
  - (b) 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
  - (c) Notify User in accordance with Section 4.01 of any Event or Breach of Confidential Information of which the Person discovers or should have discovered with the exercise of reasonable diligence. **45 CFR 164.504(e)(4)(ii)(B)**

**(O)** Except as otherwise limited by this DUA, User will, if requested by CoC Lead and HMIS Lead, use PHI to provide data aggregation services to CoC Lead and HMIS Lead, as that term is defined in the HIPAA, 45 C.F.R. §164.501 and permitted by HIPAA. **45 CFR 164.504(e)(2)(i)(B)**

**(P)** User will, on the termination or expiration of this DUA, at its expense, return to CoC Lead and HMIS Lead or Destroy, at CoC Lead and HMIS Lead's election, and to the extent reasonably

feasible and permissible by law, all Confidential Information received from CoC Lead and HMIS Lead or created or maintained by User or any of User's agents or Subcontractors on CoC Lead and HMIS Lead's behalf if that data contains Confidential Information. User will certify in writing to CoC Lead and HMIS Lead that all the Confidential Information that has been created, received, maintained, used by or disclosed to User, has been Destroyed or returned to CoC Lead and HMIS Lead, and that User and its agents and Subcontractors 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 CoC Lead and HMIS Lead 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 will immediately notify CoC Lead and HMIS Lead of the reasons such return or Destruction is not feasible, the protections of this DUA shall extend indefinitely to the Confidential Information and limit its further uses and disclosures to the purposes that make the return of the Confidential Information not feasible for as long as User maintains such Confidential Information. **45 CFR 164.504(e)(2)(ii)(J)**

**(Q)** User will create, maintain, 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. **45 CFR 164.306; 164.530(c)**

**(R)** If User accesses, transmits, stores, and/or maintains Confidential Information, User will comply with periodic security controls compliance assessment and monitoring by as CoC Lead and HMIS Lead required by state and federal law, based on the type of Confidential Information User creates, receives, maintains, uses, discloses or has access to and the Authorized Purpose and level of risk. User's security controls will be based on the National Institute of Standards and Technology (NIST) Special Publication 800-53, as amended or revised. User will update its security controls assessment whenever there are significant changes in security controls for Confidential Information and will provide the updated document to CoC Lead and HMIS Lead. CoC Lead and HMIS Lead also reserves the right to request updates as needed to satisfy state and federal monitoring requirements. **45 CFR 164.306**

**(S)** User will establish, implement and maintain any and all appropriate procedural, administrative, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, and with respect to PHI, as described in the HIPAA Privacy and Security Regulations, or other 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. **45 CFR 164.308 (administrative safeguards); 164.310 (physical safeguards); 164.312 (technical safeguards); 164.530(c)(privacy safeguards)**

**(T)** User will designate and identify, a Person or Persons, as Privacy Official **45 CFR 164.530(a)(1)** and Information Security Official, each of whom is authorized to act on behalf of User and is responsible for the development and implementation of the privacy and security requirements in this DUA. User will provide name and current address, phone number and e-mail address for such designated officials to CoC Lead and HMIS Lead upon execution of this DUA and prior to any change. **45 CFR 164.308(a)(2)**

**(U)** User represents and warrants 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 pursuant to this DUA, and further, that each has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in this DUA. **45 CFR 164.502; 164.514(d)**

**(V)** User and its Subcontractors will maintain an updated, complete, accurate and numbered list of Authorized Users, their signatures, titles and the date they agreed to be bound by the terms of this

DUA, at all times and supply it to CoC Lead and HMIS Lead, as directed, upon request.

**(W)** User will implement, update as necessary, and document reasonable and appropriate policies and procedures for privacy, security and Breach of Confidential Information and an incident response plan for an Event or Breach, to comply with the privacy, security and breach notice requirements of this DUA prior to conducting work under the DUA. **45 CFR 164.308; 164.316; 164.514(d); 164.530(i)(1)**

**(X)** User will produce copies of its information security and privacy policies and procedures and records relating to the use or disclosure of Confidential Information received from, created by, or received, used or disclosed by User under or in connection with this Agreement, within one (1) business day after request by CoC Lead and HMIS Lead or other agreed upon time frame. **45 CFR 164.308; 164.514(d)**

**(Y)** User will make available to CoC Lead and HMIS Lead any information CoC Lead and HMIS Lead requires to fulfill CoC Lead and HMIS Lead 's obligations to provide access to, or copies of, PHI in accordance with HIPAA and other applicable laws and regulations relating to Confidential Information. User will provide such information in a time and manner reasonably agreed upon or as designated by the Secretary, or other federal or state law. **45 CFR 164.504(e)(2)(i)(I)**

**(Z)** User will 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 or otherwise protected as required by rule, regulation or law. Confidential Information *at rest* requires Encryption unless there is adequate administrative, technical, and physical security, or as otherwise protected as required by rule, regulation or law. All electronic data transfer and communications of Confidential Information will be through secure systems. Proof of system, media or device security and/or Encryption must be produced to CoC Lead and HMIS Lead no later than 48 hours after CoC Lead and HMIS Lead 's written request in response to a compliance investigation, audit or the Discovery of an Event or Breach. Otherwise, requested production of such proof will be made as agreed upon by the Parties. De-identification of Confidential Information is a means of security. With respect to de-identification of PHI, "secure" means de-identified according to HIPAA Privacy standards and regulatory guidance. **45 CFR 164.312; 164.530**

**(AA)** User will comply with the following laws and standards as amended or revised *if applicable to the type of Confidential Information and the Authorized Purpose*:

- Title 1, Part 10, Chapter 202, Subchapter B, Texas Administrative Code;
- The Privacy Act of 1974;
- OMB Memorandum 07-16;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) as defined in the DUA;
- 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; and
- Any other State or Federal law, regulation, or administrative rule relating to the specific CoC Lead and HMIS Lead program area that User supports on behalf of CoC Lead and HMIS Lead.

**(BB)** User will comply with HMIS Acceptable Use standards, which require User and its employees, contractors, consultants, representatives, 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.

#### **ARTICLE 4. BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENT**

##### **Section 4.01. Breach or Event Notification to CoC Lead and HMIS Lead. 45 CFR 164.400-414**

**(A)** User will cooperate fully with CoC Lead and HMIS Lead in investigating, mitigating to the extent practicable and issuing notifications directed by CoC Lead and HMIS Lead, for any Event or Breach of Confidential Information to the extent and in the manner determined by CoC Lead and HMIS Lead.

**(B)** User's obligation begins at the Discovery of an Event or Breach and continues as long as related activity continues, until all effects of the Event are mitigated to CoC Lead and HMIS Lead's satisfaction (the "incident response period"). **45 CFR 164.404**

**(C)** Breach Notice:

(1) Initial Notice.

(a) For federal information, including without limitation, Federal Tax Information, Social Security Administration Data, and Medicaid Client Information, within the first, consecutive clock hour of Discovery, and for all other types of Confidential Information not more than 24 hours after Discovery, **or in a timeframe otherwise approved by CoC Lead and HMIS Lead in writing**, initially report to Haven's Legal Department at: legal@havenforhope.org; and **IRS Publication 1075; Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a; OMB Memorandum 07-16.**

(b) Report all information reasonably available to User about the Event or Breach of the privacy or security of Confidential Information. **45 CFR 164.410**

(c) Name, and provide contact information to CoC Lead and HMIS Lead for, User's single point of contact who will communicate with CoC Lead and HMIS Lead both on and off business hours during the incident response period.

(2) 48-Hour Formal Notice. No later than 48 consecutive clock hours after Discovery, or a time within which Discovery reasonably should have been made by User of an Event or Breach of Confidential Information, provide formal notification to CoC Lead and HMIS Lead, including all reasonably available information about the Event or Breach, and User's investigation, including without limitation and to the extent available: **For (a) -**

***(m) below: 45 CFR 164.400- 414***

- (a) The date the Event or Breach occurred;
- (b) The date of User's and, if applicable, Subcontractor's Discovery;
- (c) A brief description of the Event or 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, to the extent known or can be reasonably determined by User at that time;
- (g) User's initial risk assessment of the Event or Breach demonstrating whether individual or other notices are required by applicable law or this DUA for CoC Lead and HMIS Lead 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 CoC Lead and HMIS Lead's approval as to the steps Individuals and/or User on behalf of Individuals, should take to protect the Individuals from potential harm, including without limitation 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 Event or Breach;
- (k) Identify, describe or estimate of the Persons, Workforce, Subcontractor, or Individuals and any law enforcement that may be involved in the Event or Breach;
- (l) A reasonable schedule for User to provide regular updates to the foregoing in the future for response to the Event or Breach, but no less than every three (3) business days or as otherwise directed by CoC Lead and HMIS Lead, 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 an Event or Breach that CoC Lead and HMIS Lead requests following Discovery.

**Section 4.02. Investigation, Response and Mitigation. For A-D below: 45 CFR 160.308, 310 and 312; 160.530**

- (A) User will immediately conduct a full and complete investigation, respond to the Event or Breach, commit necessary and appropriate staff and resources to expeditiously respond, and report as required to and by CoC Lead and HMIS Lead for incident response purposes and for purposes of CoC Lead and HMIS Lead's compliance with report and notification requirements, to the satisfaction of CoC Lead and HMIS Lead

(B) User will complete or participate in a risk assessment as directed by CoC Lead and HMIS Lead following an Event or Breach, and provide the final assessment, corrective actions and mitigations to CoC Lead and HMIS Lead for review and approval.

(C) User will fully cooperate with CoC Lead and HMIS Lead to respond to inquiries and/or proceedings by state and federal authorities, Persons and/or Individuals about the Event or Breach.

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

**Section 4.03. Breach Notification to Individuals and Reporting to Authorities. Tex. Bus. & Comm. Code §521.053; 45 CFR 164.404 (Individuals), 164.406 (Media); 164.408 (Secretary)**

(A) CoC Lead and HMIS Lead may direct User to provide Breach notification to Individuals, regulators or third-parties, as specified by CoC Lead and HMIS Lead following a Breach.

(B) User must obtain CoC Lead and HMIS Lead's prior written approval of the time, manner and content of any notification to Individuals, regulators or third-parties, or any notice required by other state or federal authorities. Notice letters will be in User's name and on User's letterhead, unless otherwise directed by CoC Lead and HMIS Lead, 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 will provide CoC Lead and HMIS Lead with copies of distributed and approved communications.

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

If CoC Lead and HMIS Lead delegates notice requirements to User, CoC Lead and HMIS Lead shall, in the time and manner reasonably requested by User, cooperate and assist with User's information requests in order to make such notifications and reports.

**ARTICLE 5. GENERAL PROVISIONS**

**Section 5.01. Ownership of Confidential Information**

User acknowledges and agrees that, as between the Parties, Confidential Information is and will remain the property of CoC Lead and HMIS Lead. User agrees it acquires no title or rights to the Confidential Information.

**Section 5.02. CoC Lead and HMIS Lead Commitment and Obligations**

CoC Lead and HMIS Lead 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 CoC Lead and HMIS Lead.

**Section 5.03. CoC Lead and HMIS Lead Right to Inspection**

At any time upon reasonable notice to User, or if CoC Lead and HMIS Lead determines that User has violated this DUA, CoC Lead and HMIS Lead, 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.

**Section 5.04. Term; Termination of DUA; Survival**

(A) **Term.** Unless terminated earlier under Article 5.04(B) or (C), this DUA shall begin on the Effective Date and continue for one (1) year, when it will automatically expire (unless extended by written agreement of the Parties).

(B) **Termination by CoC Lead and HMIS Lead.** Despite any other provision, CoC Lead and HMIS Lead may terminate this DUA without cause at any time upon giving thirty (30) days prior written notice to User.

(C) **Termination for Cause.** Upon CoC Lead and HMIS Lead's sole reasonable determination that User has breached a material term of this DUA, CoC Lead and HMIS Lead shall be entitled, in its sole discretion, to do any one or more of the following:

- (1) Give User written notice of the existence of such breach and give User an opportunity to cure upon mutually agreeable terms. If User does not cure the breach or end the violation according to such terms, or if CoC Lead and HMIS Lead and User are unable to agree upon such terms, CoC Lead and HMIS Lead may immediately terminate this DUA, and seek relief in a court of competent jurisdiction in Bexar County, Texas. Simultaneously, CoC Lead and HMIS Lead may immediately stop all further disclosure of Confidential Information;
- (2) Exercise any of its rights including but not limited to reports, access and inspection under this DUA; and/or
- (3) Require User to submit to a corrective action plan, including a plan for monitoring and reporting, as CoC Lead and HMIS Lead may determine necessary to maintain compliance with this DUA and the law.

(D) **Effect of Termination.** Termination or Expiration of this DUA will not relieve User of its obligation to return or Destroy the Confidential Information as set forth in this DUA and to continue to safeguard the Confidential Information until such time as determined by CoC Lead and HMIS Lead. The duties of User or its Subcontractor under this DUA survive the termination or expiration of this DUA until all the Confidential Information is Destroyed or returned to CoC Lead and HMIS Lead, as required by this DUA. All rights, remedies, obligations, claims and liabilities which have accrued under this DUA or applicable law prior to the date on which this DUA terminates or expires shall survive such termination or expiration.

**Section 5.05. Governing Law, Venue and Litigation**

(A) The validity, construction and performance of this DUA and the legal relations among the Parties to this DUA will be governed by and construed in accordance with the laws of the State of Texas.

(B) The Parties agree that the courts of Bexar County, Texas, will be the exclusive venue for any litigation, special proceeding or other proceeding as between the parties that may be brought, or arise out of, or in connection with, or by reason of this DUA.

### **Section 5.06. Injunctive Relief**

(A) User acknowledges and agrees that CoC Lead and HMIS Lead may suffer irreparable injury if User or any of its Subcontractors 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 CoC Lead and HMIS Lead for User's or its Subcontractor's failure to comply. Accordingly, User agrees that CoC Lead and HMIS Lead 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 5.07. Indemnification**

**User will indemnify, defend and hold harmless CoC Lead, HMIS Lead and their respective employees, officers, directors, subcontractors, agents, representatives, or other members of its 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, Subcontractors, or agents or other members of its Workforce. Upon demand, User will reimburse CoC Lead and HMIS Lead for any and all losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third 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. This indemnity is independent of User's duty to procure insurance.**

### **Section 5.08. Insurance**

(A) At CoC Lead and HMIS Lead option, CoC Lead and HMIS Lead may require User to maintain, at its expense, the special and/or custom first- and third-party insurance coverages, including without limitation data breach, cyber liability, crime theft and notification expense coverages, with policy limits sufficient to cover any liability arising under this DUA, naming CoC Lead and HMIS Lead, as additional named insureds and loss payees, with primary and non-contributory status, with required insurance coverage, by the Effective Date, or as required by CoC Lead and HMIS Lead.

(B) User will provide CoC Lead and HMIS Lead with written proof that required insurance coverage is in effect, upon request.

### **Section 5.09. Fees and Costs**

Except as otherwise specified in this DUA, including but not limited to requirements to insure and/or indemnify CoC Lead and HMIS Lead, if any legal action or other proceeding is brought for the enforcement of this DUA, or because of an alleged dispute, contract violation, Event, Breach, default, misrepresentation, or injunctive action, in connection with any of the provisions of this DUA, each Party will bear their own legal expenses and the other cost incurred in that action or proceeding.

**Section 5.10. Entirety of the Contract**

This DUA constitutes the entire agreement between the Parties concerning the subject matter. 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 5.11. Automatic Amendment and Interpretation**

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

**Section 5.12. Third Party Beneficiaries**

The Third Parties are third party beneficiaries of this Agreement but have no obligations whatsoever hereunder and nothing herein shall create any such obligations (either express or implied) on the part of the Third Parties. There are no other third party beneficiaries of this Agreement.

**Section 5.13. Notices**

All notices pursuant to this DUA must be in writing and may be delivered U.S. mail or by email, and are effective on the third business day after deposit if sent by U.S. mail and if sent by email, shall be effective when received during normal business hours, to the below Notice contact information.

HMIS Lead: Haven for Hope of Bexar County  
Attn: Haven Legal Department  
1 Haven for Hope Way  
TC Bldg 3 – Admin  
San Antonio, Texas 78207  
Email: legal@havenforhope.org

CoC Lead: Close to Home  
Attn: Executive Director  
4100 E. Piedras  
Suite 105  
San Antonio, Texas 78228  
Email: katie.wilson@closetohomesa.org

User:

Attn:

Email:

**Section 5.14. Publications**

CoC Lead and HMIS Lead acknowledge that User is receiving Data Request in anticipation of preparation and publication of scholarly papers (“Scholarly Work”). User is permitted to share data with publishers if the data is de-identified in accordance with the HIPAA Safe Harbor method detailed in §164.514(b). Prior to publication of any Scholarly Work, CoC Lead and HMIS Lead will have a thirty-day period to review the publication for any disclosure of Data Request. CoC Lead and HMIS Lead shall, within the thirty-day period, give User notice identifying specifically any portion of the Data Request it believes would be impermissibly contained in the Scholarly Work, for instance but without limitation, the disclosure of personally-identifiable information or the re-identification of previously de-identified information.

**Section 5.14. Counterparts**

This DUA may be executed in one or more counterparts (including facsimile or portable document/“pdf” counterparts), each of which will be deemed an original and part of the same document.

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

**CLOSE TO HOME**

**By:** \_\_\_\_\_  
Name:  
Title:

**Date:** \_\_\_\_\_

**USER:**

**By:** \_\_\_\_\_  
Name:  
Title:

**Date:** \_\_\_\_\_

**Exhibit A**  
**Data Request**

[User Insert Scope of Data Request and Scholarly Work]