Oahu Homeless Management Information System (HMIS) & Coordinated Entry System (CES) Participation Agreement

_____(agency name), hereafter known as "Agency," hereby enters in this *Participation Agreement (PA)* regarding access and use of the Oahu Homeless Management Information System, hereafter known as "HMIS."

I. BACKGROUND AND PURPOSE

The Homeless Management Information System (HMIS) is the information system designated by the Oahu Continuum of Care (CoC) to comply with HUD's data collection, management, and reporting standards and used to collect client-level data and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness.

The U.S. Department of Housing and Urban Development (HUD) and other planners and policymakers at the federal, state and local levels use aggregate HMIS data to obtain better information about the extent and nature of homelessness over time. Specifically, an HMIS can be used to produce an unduplicated count of homeless persons, understand patterns of service use, and measure the effectiveness of homeless programs. Through the HMIS, CoC programs and clients benefit from improved internal and external coordination that guides service and systems planning. A robust HMIS also helps communities engage in informed advocacy efforts, including the pursuit of policies that result in targeted services. Analysis of information gathered through HMIS is critical to accurately calculate the size, characteristics, and needs of different subpopulations. Additionally, use of the HMIS by agencies not funded by HUD provides benefits to both these agencies and the homeless provider community at large, including the avoidance of service duplication through the sharing of client data and program enrollments. HMIS participation also positions agencies for future funding, as many private foundations now require it.

II. GENERAL PROVISIONS

A. AGREEMENT, UNDERSTANDING AND RESPONSIBILITIES

The CoC has designated Partners in Care (PIC) as the HMIS Lead Agency. All homeless assistance and homelessness prevention service providers in this CoC are eligible to become HMIS Partner Agencies, except for domestic violence providers covered by the Violence Against Women Act (VAWA).

The parties share a common interest in serving the homeless population and those at risk of becoming homeless while reducing the current number of homeless in the CoC service area. The purpose of this PA is to set out the provisions for the implementation, maintenance, coordination, and operation of the HMIS.

The Lead is responsible for administering the HMIS on behalf of the CoC, including the implementation, project management, training, maintenance, help desk support and the enhancement and upgrading of the HMIS software in coordination with the HMIS Software Provider and/or the HMIS Administrator. The Partner Agency is responsible for entering client data in the HMIS according to program type requirements. Detailed responsibilities are listed in sections below.

B. SCOPE

This PA addresses the respective responsibilities of Lead and the Partner Agency for ongoing HMIS service and activities. The specific responsibilities of the parties to this agreement for the confidentiality, reporting requirements, training, policies and procedures, hardware and software for the HMIS are clearly defined herein to ensure an effective, efficient, and secure system. All documents and addendums referenced in this agreement are also part of the agreement. Lead will abide by all applicable laws, and the Partner Agency will be expected to do the same.

III. HMIS LEAD DUTIES AND RESPONSIBILITIES

The HMIS Lead shall:

A. GENERAL

1) In consultation with its CoC, select the HMIS Software Provider, execute and manage the contract with the Software Provider, define the HMIS program and implement its standards, promote awareness of the program to all interested parties, and monitor the program's successes and failures in order to validate its effectiveness.
2) Be the sole liaison between the Partner Agency and the HMIS Software Provider; user questions concerning the software are to be directed only to the Lead and/or CoC HMIS Administrator.
3) Develop, implement, and maintain privacy, confidentiality, and security protocols for the HMIS.
4) In collaboration with the CoC HMIS Administrator, provide a standard HMIS training and technical support package to all Partner Agencies.
5) In collaboration with the HMIS Software Provider and CoC HMIS Administrator, take all necessary precautions to prevent any destructive or malicious programs from being introduced to the HMIS and, through it, to the Partner Agencies. The aforementioned entities will employ all appropriate measures to detect virus infection and all appropriate resources to efficiently disinfect any affected systems as quickly as possible.
6) In collaboration with the CoC HMIS Administrator, notify the Partner Agency of HMIS failure, errors, and/or problems immediately upon discovery.
7) In consultation with its CoC, procure, select, execute and manage a contract with the HMIS Administrator.
8) In collaboration with the CoC HMIS Administrator, provide and ensure access to help desk services on business days from 8 a.m. to 5 p.m.
9) Provide all other reasonably expected activities regarding the operation of the HMIS.

B. PRIVACY, CONFIDENTIALITY AND SECURITY

1) Maintain all client-identifying information in strictest confidence, using the latest available technology. The Lead may suspend HMIS access to any user or Partner Agency for the purpose of investigating suspicion of breached confidentiality.
2) Ensure HMIS Software Provider maintains and administers central and backup server operations including security procedures and daily system backup to prevent the loss of data.
3) Ensure the CoC HMIS Administrator monitors access to the HMIS in order to detect violations of information security protocols and maintain for inspection accurate logs of all changes made to the information contained within the database.
4) Ensure the CoC HMIS Administrator issues user accounts, passwords, and certificates of participation (when requested) for HMIS users, provided that:

a. The Partner Agency has signed the HMIS Participation Agreement,
b. The Partner Agency has paid the current year's membership fee,
c. The HMIS Lead and/or CoC HMIS Administrator has received signed HMIS User Agreements, and
d. The user has successfully completed the HMIS user training, including any related testing

5) Ensure CoC HMIS Administrator periodically changes Partner Agency passwords for security purposes and lock out user accounts after a specified period of inactivity.
6) Comply with the HMIS Privacy Policy and not release personally identifiable information to any person, agency, or organization, unless allowed by the HMIS Privacy Policy.
7) In collaboration with the CoC HMIS Administrator, set up and maintain inter-agency data sharing options in HMIS.
8) In collaboration with the CoC HMIS Administrator and CoC, conduct Partner Agency site visits to ensure compliance with privacy and security protocols.

C. USER TRAINING AND PROGRAM SETUP

1) In collaboration with the CoC HMIS Administrator and HMIS Software Provider, provide access to the initial software training for all new HMIS users.
2) In collaboration with the CoC HMIS Administrator and HMIS Software Provider, provide access to

training materials, including user manuals with definitions and instructions, to each individual who attends the training class.
3) Ensure the CoC HMIS Administrator sets up Partner Agency programs according to the HMIS Data Standards, including related grants, services, assessments, housing units, and other applicable options in the HMIS software.
4) Ensure the CoC HMIS Administrator provides access to additional trainings according to the user role, program type, or specific activities. These trainings may include classroom refreshers, reporting trainings, group webinars, one-on-one instructions, etc.
5) In collaboration with the CoC HMIS Administrator, provide other HMIS-related trainings upon request.

IV. PARTNER AGENCY DUTIES AND RESPONSIBILITIES

The Partner Agency will:

A. GENERAL

1) Be a voting member in "good standing" in your local CoC chapter.
2) Strictly adhere to all policies and procedures contained in the PA and HMIS policies and procedures, as it may be amended from time to time, and all of its appendices. (A signed hard copy of the PA will be pro-vided to the Partner Agency.)
3) Participate in and adhere to PIC CES Policies and Procedures from initial assessment to stabilized housed.
4) Subject to Hawaii Revised Statutes chapters 661 (Actions By and Against the State) and 662 (State Tort Liability Act), be liable for damages, injuries, losses, and expenses sustained by Lead, CoC and HMIS contractors as a result of the acts or omissions of the Partner Agency, its officers and employees while in the scope of employment.
5) Maintain at least two active user accounts at any one time and designate no more than two points of contact (POC) for HMIS related communication and issues.

B. PRIVACY AND CONFIDENTIALITY

1) Comply with all federal and state laws and regulations, and with all HMIS policies and procedures (particularly the HMIS Data and Technical Standards final and revised notices from HUD as may be amended from time to time, relating to the collection, storage, retrieval, and dissemination of client information).
2) Comply with the HMIS Privacy Policy and the HMIS Data Sharing Policy in the HMIS Policies and Procedures, as may be amended from time to time.
3) Obtain client consent before any data is shared. The consent to share must be:
   a. Written and signed on a HMIS Client Consent form and kept in a local file.
   b. The agency must post a visible privacy notice at the service site and/or provide a copy of the privacy notice to clients as needed.
4) Collect and maintain records of all HMIS Client Consent and other relevant documents and follow data collection protocols in accordance with the HMIS policies and procedures.
5) Take all necessary precautions to prevent destructive or malicious programs (including but not limited to viruses or spyware) from being introduced to any part of the HMIS, including users' computers. Employ appropriate measures to detect virus or spyware infection and deploy all appropriate resources to effi-ciently disinfect any affected systems as quickly as possible.

C. DATA QUALITY AND MONITORING

1) Get familiar and fully comply with the latest HMIS Data Quality Plan in the HMIS Policies and Procedures, as may be amended from time to time. The latest version is posted on the Partners In Care website and available in hard copy upon request.
2) Enter data into the HMIS within the timeframe as specified in the Data Quality Plan. Timely data entry prevents duplication of client records and other shared transactions, such as enrollments and services. It also allows good quality data for both program-specific and aggregate reports. Partner Agencies and their HMIS users may be held liable in the event that a preventable duplication occurs as a result of missing, late, or incomplete data entry. Repetitive lack of timely entry can result in official reports of concern and possible

findings against the Partner Agency and could culminate in official penalties up to and including loss of project funding and/or suspension from HMIS.

3) Collect all HUD mandatory data elements, according to the data completeness and accuracy require-ments.
4) Take all steps reasonably necessary to verify the information provided by clients for entry into the HMIS, and to see that it is correctly entered into the HMIS by the Partner Agency user.
5) Immediately notify the Lead when a programmatic, personnel, or other issue arises that precludes the Partner Agency from entering the HMIS data within the allowed timeframe. By informing the Lead in a timely fashion, the Lead and the Partner Agency can work together to craft an interim solution that is mini-mally disruptive to the HMIS as a whole.
6) Take all steps reasonably necessary to insure that no profanity, offensive language, malicious information or discriminatory comments based on race, ethnicity, religion, national origin, disability, age, gender, or sexual orientation are entered into the HMIS.
7) Not upload material into the HMIS that is in violation of any federal or state regulations, including, but not limited to: copyrighted material, material legally judged to be threatening or obscene, and material known to the Partner Agency to be confidential trade secrets.
8) Allow the Lead staff and/or CoC HMIS Administrator to conduct periodic monitoring and reviews of the original documentation in client files to ensure data accuracy. This monitoring is limited only to the client information relevant to HMIS data collection.

D. TRAINING

1) Ensure that each Partner Agency HMIS user has attended the appropriate training, has signed the HMIS User Agreement and agreed to it, and has been authorized by the Lead to access the system in accordance with the HMIS policies and procedures.
2) Ensure that the Partner Agency program managers or assigned HMIS Points of Contact (POC's) attend HMIS related meetings if requested or other Lead-sponsored HMIS trainings as required, to stay current with the HMIS policies and procedures or latest HMIS enhancements, and relate this updated information to all HMIS users at his/her Partner Agency.
3) Assess the HMIS users' data entry or reporting skills and sign up for additional training as needed.

E. SECURITY

1) Limit HMIS access only to authorized users and follow all HMIS protocols for monitoring those users. The Lead reserves the right to terminate access to any HMIS user who breaches client confidentiality or system security protocols.
2) Do not permit any person to enter or use the HMIS unless and until:
   a. The person has completed the required HMIS training,
   b. The Lead and/or CoC HMIS Administrator has issued that person the appropriate user account and Password, and
   c. Both the PA and the HMIS User Agreement have been signed and returned to the Lead and/or CoC HMIS Administrator.
3) Maintain copies of all HMIS User Agreements signed by Partner Agency personnel to whom user accounts have been issued.
4) Designate a staff person to act as the Partner Agency security officer, responsible for the implementation of the HMIS security procedures at the Partner Agency level.
5) Fully comply with the HMIS Data Sharing Policy and the HMIS Privacy Policy.
6) Not release any HMIS data to any person or organization that is not part of the HMIS, unless such release is covered by the HMIS Data Sharing Policy or the HMIS Privacy Policy.
7) Develop an internal procedure to be used in the event of a violation of any of the HMIS security protocols.
8) Develop and adhere to local security standards that should include the following:
   a. Products: Physical security (door locks, computer screen view, local network passwords, firewall)
   b. People: Personnel security (authorized users only, local oversight of usage)
   c. Procedures: Organizational security (policies and procedures are in place)
9) Notify the Lead and/or CoC HMIS Administrator within one (1) business day of the separation from the Partner Agency of any employee who was a user of the HMIS. Notification should preferably occur by close of business on the day of employee separation.
10) Notify the Lead immediately of any security breach that has occurred.

Term of Agreement

A. TERM

This Agency Participation Agreement becomes effective when signed by both parties and shall remain in effect unless terminated pursuant to paragraph VI B hereof.

B. TERMINATION

1) Either party has the right to terminate this PA with a 30-day prior written notice to the other party.
2) The Lead reserves the right to amend this PA with a 30-day notice sent to all Partner Agencies.
3) If either party believes the other to be in default of any one or more of the terms of this PA, that party will notify the other in writing of such default. The other party shall then have ten (10) days in which to cure such default. If such default is cured within such period, this PA will continue in effect. If such default is not cured within such period, the non-defaulting party shall have the right to declare this PA to be immediately terminated.
4) If this PA is terminated, the Lead HMIS and its remaining Partner Agencies shall retain their right to the use of all client data previously entered by the terminating Partner Agency, subject to any restrictions requested by the client, Client Consent form and any applicable federal, state, or local regulations regarding client privacy and confidentiality.

C. ADDENDUMS

The following Addendums are part of this Agency Participation Agreement:

1) HMIS Assurance
2) HMIS Fee Schedule, as amended
3) Hawaii's HMIS Policies and Procedures, as amended
4) PIC Coordinated Entry System Policies and Procedures Manual, as amended
5) HMIS Training Policies and Access Requirements

The signature of the parties hereto indicates their agreement with the above terms and conditions. By signing this agreement, parties acknowledge that they have read and understand this Participation Agreement and Hawaii's HMIS Policies and Procedures and all of its appendixes.

AGENCY NAME

_____

AGENCY CEO/
EXECUTIVE DIRECTOR **DATE**

_____ _____

PRINT NAME

HMIS LEAD ORGANIZATION

By_____ _____

ADMINISTRATOR

_____

PRINT NAME

Hawaii Homeless Management Information System

ASSURANCE

_____ (Name of Agency) assures that the following fully executed documents will be on file and available for review.

- ❑ A completed *HMIS Agency Request*
- ❑ The Agency's Board Approved Confidentiality Policy.
- ❑ The Agency's official *Privacy Notice* for HMIS clients.
- ❑ The Agency's official *Client Consent* form for HMIS clients.
- ❑ Confirmation that Agency's written procedures and forms follow all applicable laws, including any Agency specific regulations.
- ❑ Original HMIS *Client Consent* forms kept secure (if not a new Agency).
- ❑ Confirmation of attendance of required training for all Agency HMIS Users (if not a new Agency)
- ❑ Completed HMIS *User Agreements* for all Authorized Agency Users of HMIS.
- ❑ The Agency's official Security Plan regarding data and a completed Security Certification Checklist (Appendix 5 of *HMIS Policies and Procedures Manual*)
- ❑ A copy of the most current Hawaii specific HMIS *Policy and Procedures Manual*.

By: _____

Title: _____

Signature: _____

Date: _____