# HEART OF TEXAS HOMELESS MANAGEMENT INFORMATION SYSTEM

## Policies and Standard Operating Procedures

# CONTENTS

# SUMMARY OF POLICIES AND PROCEDURES FOR USERS

| Policy | Procedure | Section Reference for Description |
|---|---|---|
| **User Licenses:**<br>All users must sign a User Confidentiality Agreement before accessing the HoT HMIS. | The Agency Administrator must give each user a copy of the HoT HMIS Policies & Standard Operating Procedures and ensure that the user has been properly trained in both the Policies & Standard Operating Procedures and the HoT HMIS software before a user is granted access to the system.<br><br>A signed copy of the user agreement is to be kept on file at the office of the HoT HMIS Administrator.<br><br>The Agency Administrator is required to revoke the user license and access of any user upon termination of employment and immediately notify HoT HMIS Administrator. | User access Levels<br>Section A.4<br><br>Ethical Use of Data<br>User Agreements<br>Section A.9<br><br>User Licenses<br>Section B.2 |
| **Communication:**<br>Users are responsible for communicating any and all problems or concerns about the HoT HMIS to his/her Agency Administrator. | It is required that each agency designate a staff person to act as the Agency Administrator. The Agency Administrator, who receives special training, should receive questions from his/her users. When a question cannot be answered by the Agency Administrator or if the Agency Administrator is unavailable, he/she may call upon the HMIS Administrator. | Communication Sections A.5 and A.6 |
| **Data Sharing:**<br>HoT HMIS is operated under an open data sharing system. | HoT HMIS operates as an open system; electronic data sharing between agencies is permitted and encouraged. Therefore, a Release of Information (ROI) is required for each client entered into the system.<br><br>Users that are found to be inappropriately accessing and/or sharing client records will have their | Data Sharing<br>Section A.8<br><br>Profile Information<br>Section C.4 |

| | | |
|---|---|---|
| | access to the HoT HMIS immediately terminated. | |
| **Client Rights, Consent, and Ethical Use of Data:**<br>Each agency and user must abide by the terms of the agency privacy policy and the HoT HMIS Policy & Standard Operating Procedures. | Personal information collected about the persons served within programs should be protected at all times. Misuse of this data can result in the termination of access to the HoT HMIS and/or personnel action by the agency or client.<br><br>Each agency must have a privacy posting at the point of intake for review by clients. The HoT HMIS also requires the client to read and sign the ROI. Client refusal to provide information or otherwise participate in HMIS shall not be reason to deny eligibility or services. | Ethical Use of Data<br>Client Rights and Consent<br>Sections A.9 and A.11<br><br>Client Consent<br>Section D.2<br>(Attachment C) |
| **Data Removal, Review and Grievances:**<br>A client may request to see their HMIS data or may request that personally identifying information be removed from the HMIS. | Clients may follow the Agency's Grievance policy on issues related to HMIS. Grievances related to HMIS that cannot be addressed at the agency level may be escalated in writing to the HoT HMIS Committee or HoT Homeless Coalition.<br><br>In response to a legitimate request from a client to remove his/her personally identifying information from the HMIS, the agency should remove such data from the client record within 72 hours. A record of these transactions must be kept by the Agency Administrator. In response to requests to view his/her data in the HMIS, the agency administrator or case manager must provide a copy of the requested data within a reasonable time frame to the client. Requests for changes to client information are considered on a case by case basis. | Client Grievances<br>Section A.13<br><br>Data Retrieval, Client<br>Section D.11 |

| | | |
|---|---|---|
| **Security and User Access:** Each user is provided with a unique user name and password. | Sharing of user names and passwords is prohibited in the HoT HMIS. Sharing of user name and/or passwords is considered a serious breach of the user agreement and could result in sanctions and/or appropriate personnel action. | Security Section B.1 (Attachment B) |
| **Security and Data Retrieval:** Agencies must protect identified data that is downloaded or retrieved from the HMIS onto local computers and/or networks. | Once identified data has been retrieved from the HMIS and saved to a PC, network or disk, the data must be kept secure through encryption and/or password protection. Storing identified data on floppy disks, CDs, flash drives or unprotected laptops is not recommended unless proper security precautions have been taken. Unencrypted or unprotected data from the HMIS may not be sent via email. | Extracted Data Section B.5 |
| **Security Requirements for Agencies:** Because the HoT HMIS is accessed over the internet and contains personal data that must be protected, each agency is required to follow a minimum set of guidelines to ensure security of the entire system. | Each agency must have appropriate protections in place on the network and/or stand-alone PC that accesses the HoT HMIS. | Data Access Computer Requirements Section B.6 |
| **Training:** User training on a variety of HMIS topics is offered on a quarterly basis. | Although initial user training is to be conducted by the HMIS Administrator, a schedule of user training sessions on a quarterly basis in a classroom style setting is offered. Contact the HoT HMIS Administrator for the schedule of trainings available. | Training: Section C.5 |

| | | |
|---|---|---|
| **Data Collection and Data Quality:**<br>Each program is required to collect a series of data elements depending on the type of program it operates. The HoT data elements are based on HUD's Data and Technical Standards. Data entry must meet the data quality thresholds to be considered complete. | Each program must have all the required data elements in the HoT HMIS weekly. Data entry for the previous week must be completed on the following Monday.<br><br>Data quality and integrity is expected of all HMIS users. The HMIS Administrator may perform data quality reviews and require corrective action if data quality does not meet required standards. HUD-funded programs are required to submit an HMIS- generated APR every quarter. | Required Data Collection: Section D.1. (Attachment E)<br><br>https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf |
| **Program-specific HMIS Manuals** | | PATH Program HMIS Manual: https://www.hudexchange.info/resources/documents/PATH-Program-HMIS-Manual.pdf<br><br>CoC Program HMIS Manual: https://www.hudexchange.info/resources/documents/CoC-Program-HMIS-Manual.pdf<br><br>ESG Program HMIS Manual: https://www.hudexchange.info/resources/documents/ESG-Program-HMIS-Manual.pdf<br><br>RHY Program HMIS Manual: https://www.hudexchange.info/resources/documents/RHY-Program-HMIS-Manual.pdf<br><br>HOPWA Program HMIS Manual: https://www.hudexchange.info/resources/documents/HOPWA-Program-HMIS-Manual.pdf<br><br>VA Programs HMIS Manual: https://www.hudexchange.info/resources/documents/VA-Programs-HMIS-Manual.pdf |

# Policies and Standard Operating Procedures Introduction

This document details the policies, procedures, guidelines, and standards that govern the operations of the Heart of Texas Homeless Management Information System (HoT HMIS). It outlines the roles and responsibilities of all agencies and persons with access to HoT HMIS data, and it contains important and useful information about the ways in which HoT HMIS data is secured and protected. All Providers using the HoT HMIS should read this document in full and train every end user within its agency and programs to understand its contents as necessary. Attachment B is a user license agreement, which includes a statement that the user has read and understands these operating procedures.

### INTRODUCTION

The Heart of Texas Homeless Coalition (HoTHC) is a non-profit organization whose vision is stated as: "There will be no gaps in available services to homeless or otherwise qualifying individuals." The Coalition is committed to developing a seamless Continuum of Care model that will provide all homeless individuals an opportunity to access needed services. The City of Waco is the entity that provides HMIS support to the Heart of Texas Homeless Coalition and homeless provider agencies. The HoTHC and the City of Waco have established a Memorandum of Understanding (MOU) to provide and manage the HMIS for the HoT. The HoTHC and the HMIS Administrator in conjunction with the local Continuum of Care (CoC) strive to meet or exceed HUD standards in data accuracy.

HUD requires unduplicated statistical demographic reports on the numbers and characteristics of clients served as well as on program outcomes. In order to address the reporting requirements mandated by HUD, the HoT has implemented an electronic management information system that will provide the necessary demographic information and reports. This system is called the Heart of Texas Homeless Management Information System (HoT HMIS). Mediware Information Systems, Inc. is the vendor of the web-based software known as *ServicePoint,* which was selected in 2001 as part of a competitive process. The HMIS Administrator provides training and technical assistance to users of the HoT HMIS. All Providers funded by the City of Waco's Community Development Block Grant (CDBG) or that receive certain HUD grants are required to participate in the HoT HMIS. The only exception being domestic violence shelters which are prohibited by law from HMIS participation.

Providers participating in the HoT HMIS are required to collect and record certain data elements for all new and continuing clients in the HMIS weekly. Data entry should be completed weekly. All records should be up to date every Monday for clients served during the prior week. All Providers using the HoT HMIS are also required to comply with HUD's *HMIS Data and Technical Standards* (see Attachment E for an UDE overview and access to a full copy of HUD's Standards).

Maintaining confidential client records in a secure environment to ensure that the information is not misused or accessed by unauthorized people is of the utmost importance. The following Policies and Standard Operating Procedures have been developed to establish standards for the collection, storage and dissemination of confidential information by the users of the HoT HMIS. The HoT HMIS is an open system which does allow for sharing of electronic data between agencies. Programs can share information entered into the HoT HMIS. The HMIS Administrator is the only entity able to access all the client-level information,

including personal identifiers, contained in the HoT HMIS. Acceptable uses and disclosures of the data are outlined in this manual. For example, City of Waco may disclose data that is required under a court order issued by a judge, to protect the health and safety of those being served in its programs, and could use de-identified data for research and analysis purposes. Neither the City of Waco nor HUD requires client-level information from the HoT HMIS for the programs it funds. Thus only de-identified and/or aggregate-level data is shared with HUD.

## HoT HMIS Goals

The goals of the HoT HMIS are to support and improve the delivery of homeless services in the Heart of Texas. Inclusive in these goals is the improvement of the knowledge base about homelessness that contributes to an enlightened and effective public response to homelessness. The HoT HMIS is a tool that facilitates the following:

- Improvements in service delivery for clients as case managers assess the client's needs, inform the client about available services on site or through referral, help the client find and keep permanent housing, and improve service coordination when information is shared between programs and among agencies that are serving the same client
- A confidential and secure environment that protects the collection and use of all client data including personal identifiers
- The automatic generation of standard reports required by HUD, including participation in the national Annual Homelessness Assessment Report (AHAR)
- Generation of system-level data and analysis of resources, service delivery needs and program outcomes for the HoT homeless population
- A data collection and management tool for Partners to administer and supervise their programs

All users are required to recognize the need to maintain each client's confidentiality, and will treat the personal data contained within the HoT HMIS with respect and care. As the guardians entrusted with this personal data, each user has both an ethical and a legal obligation to ensure that data is collected, accessed and used appropriately. Of primary concern are issues of security and the policies governing the release of this information to the public, government, and funders. Meeting the needs of homeless persons served by HoT HMIS and its Providers is the underlying and most basic reason for having the HoT HMIS, and employing it for continued improvements in program quality.

## Definitions

Many of the terms used in this Policies and Standard Operating Procedures Handbook may be new to many users. Definitions of some of these terms are as follows:

**Agency Administrator**
The person responsible for system administration at the agency level and for notifying the HMIS Administrator of needed changes.

**Authentication**
The process of identifying a user in order to grant access to a system or resource; usually based on a username and password.

**City of Waco (lead agency)**
The entity that provides Homeless Management Information Systems (HMIS) support to the Heart of Texas Homeless Coalition and homeless provider agencies.

**Client**
Any recipient of services offered by a Provider or Partner.

**Client-level Data**
Data collected or maintained about a specific person, this type of data can be de-identified for purposes of data analysis, which means that personally identifying information is removed from the record.

**Continuum of Care (CoC)**
Governing entity to oversee the implementation of HMIS.

**Database**
An electronic system for organizing data, usually organized by fields and records, so it can easily be searched and retrieved.

**De-identified Data**
Data that has been stripped of personally identifying information.

**Encryption**
Translation of data from plain text to a coded format, only those with the "key" have the ability to correctly read the data; encryption is used to protect data as it moves over the internet and at the database level through the use of special software.

**Firewall**
A method of controlling access to a private network to provide security of data; firewalls can use software, hardware, or a combination of both to control access.

**Heart of Texas Homeless Coalition (HOTHC)**
Heart of Texas Homeless Coalition is the Collaborative Applicant for the TX-604 Waco/McLennan County Continuum of Care.

**Heart of Texas Homeless Management Information System (HoT HMIS)**
The specific HMIS utilized in the Heart of Texas, currently the HoT HMIS uses software produced by Mediware Information Systems, Inc. called *ServicePoint.*

**Homeless Management Information System (HMIS)**
Homeless Management Information System; this is a generic term for any system used to manage data about homelessness and housing.

**HoT HMIS Administrator**
The job title of the person who provides technical support and training to HMIS users, this person has the highest level of user access in *ServicePoint* and has full access to all user and administrative functions.

**HUD HMIS Data and Technical Standards**
The HUD HMIS Data and Technical Standards were updated and made effective on October 1, 2017. These standards can be viewed at https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf.

**Identifying Information**
Information that is unique to an individual and that may be used to identify a specific person; examples of identifying information are name and social security number.

**Mediware Information Systems, Inc.**
Aka Mediware, the company that wrote the software used for the HoT HMIS; Mediware Information Systems, Inc. also houses and maintains the server that holds our HMIS database.

**Module**
The ServicePoint software has several sections that focus on different types of functions related to HMIS, these sections, known as "modules," include ClientPoint (for entering client data & services), ResourcePoint (for looking up homeless services), and ShelterPoint (for checking clients in and out of beds).

**Partner**
Any agency, organization or group who has an HMIS Agency Agreement and/or contract with HoT HMIS and that is allowed access to the HoT HMIS database, these Agencies connect independently to the database via the Internet.

**Provider**
Any organization under contract with HoT HMIS to provide outreach, shelter, housing, employment and/or social services to homeless people.

**Release of Information (ROI)**
A Release of Information indicates that a *ServicePoint* client has given their permission for your provider/organization/program to share their information with other providers outside of your agency.

**Server**
A computer on a network that manages resources for use by other computers in the network; for example, a file server stores files that other computers (with appropriate permissions) can access, one file server can "serve" many files to many client computers, a database server stores a data file and performs database queries for client computers.

***ServicePoint***
A web-based software package developed by Mediware Information Systems, Inc. which tracks data about people in housing crisis in order to determine individual needs and provide aggregate data for reporting and planning.

**User**
An individual who uses a particular software package; in the case of the HoT HMIS, the *ServicePoint* software

**User License**
An agreement with a software company that allows an individual to use the product, in the case of ServicePoint, user licenses are agreements between the City of Waco and Mediware Information Systems, Inc. that govern individual connections to the HoT HMIS, user licenses cannot be shared.

# A. Organization and Management of the HoT HMIS

## A.1. PROJECT MANAGEMENT

**Policy**

The City of Waco is responsible for project management and coordination of the HoT HMIS. The City of Waco employs the HoT HMIS Administrator who is responsible for all system-wide policies, procedures, communication, performance measurement reporting and coordination. The HMIS Administrator is the primary contact with Mediware Information Systems, Inc. and works with Mediware to implement any necessary or desired system-wide changes and updates. In this role as HMIS Administrator, the City of Waco endeavors to provide a uniform HoT HMIS that yields the most consistent data for client management, agency reporting and service planning.

**Procedure**

All concerns relating to the policies and procedures of the HMIS should be addressed with the HMIS Administrator, the CoC and/or the HoTHC.

## A.2. SYSTEM ADMINISTRATION

**Policy**

The City of Waco employs the HMIS Administrator whose primary responsibility is the coordination and administration of the HoT HMIS.

**Procedure**

The HoT HMIS Administrator manages day-to-day operations of the HoT HMIS and is governed by a confidentially agreement that allows access to client level data. All system-wide questions and issues should be directed to the HoT HMIS Administrator.

These operations include:

- Release of Information (ROI) for HMIS client data sharing
- Memorandum of Understanding (MOU) between City of Waco and Participating Agencies
- Data Quality Assurance Plan for Participating Agencies in HMIS
- License and support fees charged to Participating Agencies
- Reviews Technical Data Standards as published by HUD
- Organizing training and technical assistance to participating agencies on all HMIS policies and procedures related to authorizing access to the system, including agency setup, questions from users, network questions and system functionality questions;
- Overseeing system administration with concentration on internal and external security protocols;
- Monitoring access to the web based application through automated queries and software application protocols;
- Provide periodic reports from Mediware on data security and test results;
- Coordinating assistance with data analysis, findings, and report writing;
- Coordinating implementation of software enhancements; and

- Conducting training and supervising system administration functions in a way that respects the dignity of the people whose data is being collected.

HUD reports that are reviewed by the body would include:

- Point-In-Time (PIT)
- Housing Inventory Chart (HIC)
- Annual Homeless Assessment Report (AHAR)
- System Performance Report (Sys PM)

### A.3. PARTICIPATING AGENCY

**Policy**

Each Partner must designate a staff member to be the HMIS Agency Administrator who is responsible on a day-to-day basis for enforcing the data and office security requirements under these Policies and Standard Operating Procedures.

**Procedure**

The Executive Director of the Partner Agency must identify an appropriate Agency Administrator and provide that person's name and contact information to the HoT HMIS Administrator. Changes to that information over time should be reported immediately to the HoT HMIS Administrator. The HoT HMIS Administrator is responsible for maintaining a current list of Agency Administrators.
Agency Administrators are responsible for the following:

- Attends required Agency Administrator training. Must have an email address and be a licensed user
- Are responsible for the removal of licensed users from the HMIS immediately upon their employee's termination from agency, placement on disciplinary probation, or upon any change in duties not necessitating access to HMIS information, or inform the HoT HMIS Administrator immediately of the change in status.
- Is responsible for all activity associated with agency staff access and use of the HMIS data system
- Provides agency HMIS Users support and clarification on system functionality. Ensures that all authorized persons complete all required steps before obtaining access to the system and adhere to the responsibilities of an HMIS User as outlined in the Policies and Procedures Manual.
- Has access to all client data, user data and agency administration information for the Partner; thus is responsible for the quality and accuracy of this data.
- Ensures the stability of the agency connection to the Internet and *ServicePoint*, either directly or in communication with other technical professionals.
- Provides support for the generation of agency reports.
- Monitors and enforces compliance with standards of client confidentiality and ethical data collection, entry, and retrieval at the agency level.
- Reports system problems and data-related inconsistencies to HMIS System Administrator.

The Agency also oversees the implementation of data security policies and standards and will:

- Assume responsibility for integrity and protection of client-level data entered into the HMIS system;

- Ensure organizational adherence to the HMIS Policies and Procedures;
- Communicate control and protection requirements to agency custodians and users;
- Authorize data access to agency staff and assign responsibility for custody of the data;
- Ensure that data is collected in a way that respects the dignity of the participants;
- Ensure that all data collected must be relevant to the purpose for which it is used, that the data is entered accurately and on time; and
- Provide prompt and timely communications of data, changes in license assignments, and user accounts and software to the HMIS Administrator.

### A.4. AGENCY ADMINISTRATOR

**Policy**

Every Participating Agency must designate one person to be the Agency Administrator /who holds responsibility for the coordination of the system software at the agency.

**Procedure**

The Agency Administrator/Data Security Officer will be responsible for duties including:

- Editing and updating agency information;
- Ensuring that access to the HMIS is requested for authorized staff members only after they have: received training; for all user levels; satisfactorily demonstrated proficiency in use of the software; and demonstrated an understanding of the HMIS Policies and Procedures and agency policies;
- Granting technical access to the software system for persons authorized by the Agency's leadership by requesting the system administrator to create passwords needed to enter the system;
- Designating each individual's level of access;
- Ensuring new staff persons are trained on the uses of the HMIS software system, including review of the Policies and Procedures in this document and any agency policies which impact the security and integrity of client information;
- Notifying all users in their agency of interruptions in service;
- Serving as point-person in communicating with the HMIS Administrator;
- Facilitating timely reporting from the Agency;
- Working cooperatively with HMIS technical staff and consultants.

The Agency Administrator/Data Security Officer is also responsible for implementation of data security policy and standards, including:

- Administering agency-specified business and data protection controls;
- Administering and monitoring access control;
- Providing assistance in and/or coordinating the recovery of data, when necessary; and
- Detecting and responding to violations of the Policies and Procedures or agency procedures.
- Maintaining records of background checks for all persons who have been given access to the HMIS in accordance with Texas Administrative Code. (see appendix)

HMIS staff will coordinate training and technical assistance for Agency Administrator.

## A.5. USER ACCESS LEVELS

**Policy**

All HoT HMIS Users will have a level of access to HMIS data that is appropriate to the duties of their position so that information is recorded and accessed on a "need to know" basis. All users should have the level of access that allows efficient job performance without compromising the security of the HoT HMIS or the integrity of client information.

**Procedure**

Each Agency Administrator (and/or its Executive Director) will identify the level of access each licensed user will have to the HMIS database.

Responsibilities:

- The HMIS Administrator agrees to authorize use of the HMIS only to users who have received appropriate training, and who need access to the system for technical administration of the system, report writing, data analysis and report generation, back-up administration or other essential activity associated with carrying out HMIS responsibilities.
- The Participating Agency agrees to authorize use of the HMIS only to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

Users are any persons who use the HMIS software for data processing services. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the data security policy and standards as described and stated by the Agency. Users are accountable for their actions and for any actions undertaken with their usernames and passwords. Users must advise the Agency Administrator (or HMIS Administrator) if their passwords are compromised.

Contractors, volunteers, interns and others who function as staff, whether paid or not, are bound by the same User responsibilities and rules set forth in this manual.

User Levels: There are several levels of access to *ServicePoint*. These levels should be reflective of the access a user has to client level paper records and should be determined by a staff person's position in the organization, their direct interaction with clients and their data entry responsibilities.

ServicePoint access levels are described in the following table:

| SERVICEPOINT ACCESS LEVELS | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Resource Specialist 1 | Resource Specialist 2 | Resource Specialist 3 | Volunteer | Agency Staff | Case Managers 1 & 2 | Agency Admins | Executive Directors | System Operators | System Admins 1 | System Admins 2 |
| ClientPoint | | | | | | | | | | | |
| Profiles | | | | X | X | X | X | X | | X | X |
| Assessments | | | | | | X | X | X | | X | X |
| Case Notes | | | | | | X | X | X | | X | X |
| Case Plans | | | | | | X | X | X | | X | X |
| Service Records | | | | X | X | X | X | X | | X | X |
| ServicePoint | | | | | | | | | | | |
| Referrals | | | | X | X | X | X | X | | X | X |
| Services Provided | | | | | X | X | X | X | | X | X |
| ResourcePoint | X | X | X | X | X | X | X | X | X | X | X |
| ShelterPoint | | | | X | X | X | X | X | | X | X |
| Reports | | | | | | | | | | | |
| Audit Reports | | | | | | | | | | | |
| Client/Service Information | | | | | | | X | X | | X | X |
| User Information | | | X | | | | X | X | | X | X |
| Client/Service Access Information | | | | | | | | | | | |
| Provider Reports | | | | | | | | | | | |
| Client Served Report | | | | | | X | X | X | | X | & |
| Daily Bed Report | | | X | | | x | X | X | | X | X |
| Entry/Exit Report | | | | | | X | X | X | | X | & |
| Exhibit 1 Report | | | | | | | | | | | & |
| HUD 40118 APR | | | | | | X | X | X | | X | & |
| PATH Report | | | | | | X | X | X | | X | & |
| Outstanding Referral Report | | | X | | | X | X | X | | X | X |
| Service Transaction Report | | | | | | X | X | X | | X | X |
| Needs Report | | | | | | X | X | X | | X | & |
| ReportWriter | | | | | | X | X | X | | X | X |
| Administration | | | | | | | | | | | |
| Add/Edit Users | | | | | | | X | X | X | X | X |
| Reset Passwords | | | | | | | X | X | X | X | X |

| | Resource Specialist 1 | Resource Specialist 2 | Resource Specialist 3 | Volunteer | Agency Staff | Case Managers 1 & 2 | Agency Admins | Executive Directors | System Operators | System Admins 1 | System Admins 2 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Add Provider | | | X | | | | | | X | X | X |
| Agency News | | X | X | | X | X | X | X | X | X | X |
| System News | | | X | | | | | | X | X | X |
| Provider Groups | | | | | | | | | | | |
| Picklist Data | | | | | | | | | X | X | X |
| Licenses | | | | | | | | | X | X | X |
| Assessment Admin | | | | | | | | | X | X | X |
| Shadow Mode | | | | | | | | | | | X |
| System Preferences | | | | | | | | | | | X |

X - Users have access to this section of ServicePoint
O - Users can neither delete the Provider they belong to, nor any of their Parent Providers.
# - Users cannot edit their Parent Provider, they may edit their own Provider or their Child Providers only.
+ - Users can run the report for Provider Groups.

## A.6. TRAINING SCHEDULE

HMIS staff will coordinate ongoing training schedules for Systems Administrators, Agency Administrators and End Users. Training will occur on a regular basis. The schedule of trainings will be published by HOTHC/HMIS Staff.

**Training schedule**

Ethics and Compliance Training:

- Mandatory
- Review of Ethics
- Review of Compliance around Privacy and HIPAA laws and regulations

New User Training - Introduction to the HMIS System (End User Training):

- Introduction to the HMIS Project
- Review of applicable policies and procedures each year
- Logging on to the HMIS System
- Entering client information including Universal Data Elements, Program specific elements, demographics, Entry/Exits, and service transactions

Job Function Training:

- Intake Worker
- Resource Specialist
- Activity Specialist
- Case Manager
- Program Manager
- Executive Director

Agency Administrator Training:

- Six hours mandatory
- Review of agency roles and responsibilities
- Review of security policies and procedures
- Overview of system administrative functions
- Entering and updating information pertaining to the participating agency
- Review of HMIS technical infrastructure
- Reporting

Annual recertification of training required based on job/administration function.

## A.7. COMMUNICATION WITH PARTNERS

**Policy**

The HoT HMIS Administrator is responsible for relevant and timely communication with each agency regarding the HoT HMIS. The HoT HMIS Administrator will communicate system-wide changes and other relevant information to Agencies as needed. He/she will also maintain a high level of availability to Partners. Good

communication is essential to the proper functionality of any system, electronic or otherwise. Providing a single point of communication simplifies and speeds communications within the HoT HMIS. The HoT HMIS Administrator will also develop and maintain a listserv to facilitate communication with agency administrators.

**Procedure**

General communications from the HoT HMIS Administrator will be directed towards the Agency Administrator. Specific communications will be addressed to the person or people involved. The HoT HMIS Administrator will be available via email, phone, and mail. The message board (NewsFlash) function in ServicePoint will also be used to distribute HMIS information. While specific problem resolution may take longer, the HoT HMIS Administrator will strive to respond to Partner questions and issues within three business days of receipt. In the event of planned unavailability, the HoT HMIS Administrator will notify Partners in advance and designate a backup contact.

Information affecting all users will be directed to the Agency Administrators. Agency Administrators are responsible for distributing that information to any additional people at their agency who may need to receive it, including, but not limited to, Executive Directors, client intake workers, and data entry staff. Agency Administrators are responsible for communication with all of their agency's users. If an Agency is needing help there the agency will need to submit a HMIS Help Desk Ticket that will be address by HMIS administrator within 72 hours. If received on a weekend or Holiday the 72 hours will begin on the next regular business work day.

### A.8. COMMUNICATION WITH HOT HMIS ADMINISTRATOR

**Policy**

Partner Agencies are responsible for communicating needs and questions regarding the HoT HMIS directly to the HoT HMIS Administrator. In order to foster clarity both for HoT HMIS users and for Mediware Information Systems, Inc. ALL communications with Mediware regarding the HoT HMIS must go through the HoT HMIS Administrator. The City of Waco holds the contract with Mediware, and is therefore responsible for acting as the primary contact for the HoT HMIS. Designated points of communication within Partners and within the City of Waco to simplify and speed communications about the HoT HMIS.

**Procedure**

Users at Partner Agencies will communicate needs, issues and questions to the Agency Administrator. If the Agency Administrator is unable to resolve the issue, the Agency Administrator will contact the HoT HMIS Administrator via email, phone or mail. The HoT HMIS Administrator will attempt to respond to Partner needs within three business days of the first contact. If the HoT HMIS Administrator cannot resolve the issue, he/she may contact Mediware Information Systems, Inc. for technical assistance.

### A.9. SYSTEM AVAILABILITY

**Policy**

The City of Waco and Mediware Information Systems, Inc. will provide a highly available database server and will inform users in advance of any planned interruption in service. A highly available database affords agencies the opportunity to plan data entry, management, and reporting according to their own internal schedules. Availability is the key element in maintaining an HMIS that is a useful tool for Partners to use in managing programs and services.

**Procedure**

No computer system achieves 100% uptime. Downtime may be experienced for routine maintenance, in the event of a disaster or due to systems failures beyond the control of Mediware Information Systems, Inc. or the City of Waco. In the event of disaster or routine planned server downtime, Mediware Information Systems, Inc. will contact the HoT HMIS Administrator. The HoT HMIS Administrator will contact Agency Administrators and inform them of the cause and duration of the interruption in service. The HoT HMIS Administrator will log all downtime for purposes of system evaluation. In the event that it is needed, Mediware Information Systems, Inc. is required to have redundant systems in place so that connection to the server can be restored as quickly as possible.

### A.10. INTER-AGENCY DATA SHARING

**Policy**

The HoT HMIS is an open data sharing system. This means that clients' data will be shared among Partners within the HoT HMIS. A Release of Information (ROI) is required to be signed by each client before the information is entered into the HMIS. The ROI must be established in *ServicePoint* on the same day (or a previous date) the demographic data is entered into the system. Fields such as medical, mental health and legal stay closed at all times. Other fields, such as case management, can be closed upon request.

**Procedure**

When new clients and new service records are entered into ServicePoint, the initiating user must maintain the default setting of each record as "open" to users from other Partners.

### A.11. ETHICAL DATA USE

**Policy**

Data contained in the HoT HMIS will only be used to support or report on the delivery of homeless and housing services in the Heart of Texas. Each HMIS User will affirm the principles of ethical data use and client confidentiality contained in the HoT HMIS Policies and Standard Operating Procedures Manual and the HoT HMIS User Agreement. The data collected in the HoT HMIS is the personal information of people in the Heart of Texas community who are experiencing a housing or financial crisis. It is the user's responsibility as the guardian of that data to ensure that it is only used to the ends to which it was collected and in and the manner to which the individual client has given consent.

**Procedure**

All HoT HMIS users will sign a HoT HMIS User Agreement before being given access to the HoT HMIS. Any individual or Partner misusing, or attempting to misuse HMIS data will be denied access to the database, and his/her/its relationship HoT HMIS may be terminated.

### A.12. ACCESS TO HOT HMIS DATABASE

**Policy**

No one but Mediware Information Systems, Inc. will have direct access to the HoT HMIS database through any means other than the *ServicePoint* software.

**Procedure**

Under its contract with the City of Waco, Mediware Information Systems, Inc. will monitor both our web application server and our database server and employ updated security methods to prevent unauthorized database access. Any party who has access to the HoT HMIS database must sign a User Agreement prior to system access.

### A.13. CLIENT RIGHTS AND CONFIDENTIALITY OF RECORDS

**Policy**

The HoT HMIS operates under a protocol based on the Release of Information (ROI) to include client data in the HMIS. Each Partner is required to post a HoT HMIS Discloser in a place where clients may easily view it such as the point of intake, on a clipboard for outreach providers, in a case management office, etc. The HoT HMIS Disclosure includes a statement about the uses and disclosures of client data as outlined in this document (See Attachment D). An ROI is required in order for a client's information to be shared with other participating agencies within the HoT HMIS. Clients may opt out of HMIS or be unable to provide basic personal information. Clients have the right of refusal to provide personally identifiable information to the HMIS, except in cases where such information is required to determine program eligibility or is required by the program's funders. Such refusal or inability to produce the information shall not be a reason to deny eligibility or services to a client. When a client exercises his/her right of refusal, de-identified demographic information will be entered into the HMIS. Each Partner shall take appropriate steps to ensure that authorized users only gain access to confidential information on a "need-to-know" basis. The data in the HoT HMIS is personal data, collected from people in a vulnerable situation. The City of Waco and Partners are ethically and legally responsible to protect the confidentiality of this information. The HoT HMIS will be a confidential and secure environment protecting the collection and use of client data.

**Procedure**

Access to client data will be controlled using security technology and restrictive access policies. Each Partner must make available a privacy policy related to client data captured in HMIS. The HoT HMIS Disclosure must be placed in an area easily viewed by clients. Only individuals authorized to view or edit individual client data in accordance with the stated privacy policies and these Standard Operating Procedures will have access to that data. The HoT HMIS will employ a variety of technical and procedural methods to ensure that only authorized individuals have access to individual client data.

### A.14. PARTNER GRIEVANCES

**Policy**

Partners will contact the HoT HMIS Administrator to resolve HMIS problems including but not limited to operation or policy issues. If an issue needs to be escalated, Partners may also contact the HMIS Program Planner or Director of Housing and Economic Development at the City of Waco.

**Procedure**

Partners will bring HMIS problems or concerns to the attention of the HoT HMIS Administrator, who may ask for these issues to be stated in writing. If problems, concerns or grievances cannot be resolved by the HoT HMIS Administrator, or if it is not appropriate to raise the issue with the HoT HMIS Administrator, the issue can be directed to the Director of Housing and Economic Development. If the grievance requires further attention, the HoTHC and CoC may be notified.

## A.15. CLIENT GRIEVANCES

**Policy**

Clients must contact the Partner with which they have a grievance for resolution of HoT HMIS problems. Partners will report all HMIS-related client grievances to the HoT HMIS Administrator. If the Partner's grievance process has been followed without resolution, the Partner may escalate the grievance to HoT HMIS Administrator as outlined in Section A.12. At any time, clients may request that their personally- identifying information be removed from the HoT HMIS.

**Procedure**

Each Partner is responsible for answering questions, complaints and issues from their own clients regarding the HoT HMIS. Partners will provide a copy of their privacy policy and/or of the HoT HMIS Policies and Standard Operating Procedures Manual upon client request. Client complaints should be handled in accordance with the Partner's internal grievance procedure, and then escalated to HoT HMIS Administrator in writing if no resolution is reached. HoT HMIS Administrator is responsible for the overall use of the HoT HMIS, and will respond if users or Partners fail to follow the terms of the HoT HMIS Agency Agreement, breach client confidentiality or misuse client data. Partners are obligated to report all HMIS-related client problems and complaints to HoT HMIS Administrator, which will determine the need for further action. The HoT HMIS Administrator will record all grievances and will report these complaints to the CoC. Resulting actions might include further investigation of incidents, clarification or review of policies or sanctioning of users and Agencies if users or Agencies are found to have violated standards set forth in HoT HMIS Agency Agreements or the Policies and Standard Operating Procedures Manual. Upon the client's request for data removal from the HoT HMIS, the Agency Administrator will delete all personal identifiers of client data within 72 hours. A record of these transactions will be kept by the Agency Administrator.

## A.16. HARDWARE, CONNECTIVITY AND COMPUTER SECURITY REQUIREMENTS

**Policy**

Partners will provide their own computer and method of connecting to the Internet, and thus to the HoT HMIS. The City of Waco understands the cost and difficulty of acquiring and maintaining computers and Internet access.

**Procedure**

Contact the HoT HMIS Administrator for the current status of assistance. Hardware/Software Requirements: ServicePoint is web-enabled software; all that is required to use the database is a computer, a valid username and password, and the ability to connect to the Internet. There is no unusual hardware or additional ServicePoint-related software or other software installation required. Mediware guidelines state the following workstation specifications.

**Workstation Specifications**

The minimum desktop specifications for ServicePoint 5 are:

- Computer – PC only (Mediware does NOT officially support Macintosh).
- Mobile Devices – The only mobile device that is officially supported by Mediware is the Apple iPad running the latest version of iOS. At the time of this writing, testing has been completed with version 8.1.2. However, many mobile devices may be able to run ServicePoint, but if the device does not support Java, or does not run Java version 7 release 76, then it will not run ART. ServicePoint will not

display correctly on a screen smaller 1024 pixels wide, and may be too small to on screens less than 7 inches.

- OS/Memory
  - Windows Vista
    - As of April 11, 2017 Microsoft has ended all support for Windows Vista. As a result of the discontinued support, Microsoft is no longer providing updates to this operating system. This can result in security vulnerabilities that could render the installation unstable or even insecure. Because Microsoft is no longer supporting Windows Vista, Mediware cannot recommend using Windows Vista with ServicePoint.
  - Windows 7 – 8 GB recommended (4 GB minimum)
    - Currently, Windows 7 is the most stable operating system for both ServicePoint and ART. Both architectures, 32bit and 64bit, run ServicePoint very well. However, if running the 64bit version of Windows 7 with Chrome, be sure to use the 32bit version of Java (see Java in Browsers Section). Chrome will not run 64bit Java.
  - Windows 8 – 8 GB recommended (4 GB minimum)
    - There should be no issue with running Windows 8 as long as the most current version of Java that is installed is version Java 7 release 76. Be aware that within windows 8, there are 2 different versions of Internet Explorer. There is the "Modern" version of the browser as well as the classic "Desktop" version. The "Modern" version, that runs from the Live Tile interface, is not compatible with ART, however the classic desktop version is, as long as the proper version of Java is installed. Internet Explorer "Modern" version can cause the pop-ups to appear in difficult to read locations while in split screen mode as well as causing the browser to close unexpectedly. This is not a complete incompatibility issue, but it is a bug that can cause frustration. If the window unexpectedly closes before data can be saved, the data will have to be re-entered into the system upon re-load.
  - Windows 8 RT -- 8 GB recommended (4 GB minimum)
    - Windows 8 RT, which is a version of Windows 8 for tablet devices, is not compatible with ART. This is because there is no other browser on the operating system except for the incompatible "Modern" version of Internet Explorer. Windows 8 RT only allows apps to be installed that are available in the Windows App store. Currently, no other browser is allowed in the Microsoft App store, making the incompatible version of Internet Explorer the only browser allowed to run on Windows 8 RT. Microsoft has begun to phase out Windows RT and it is being replaced with Windows 8.1.
  - Windows 10 – 8 GB recommended (4 GB minimum)
    - Windows 10 is supported.
- Java
  - Java is a required component for the Advanced Reporting Tool (ART). However, not all versions of Java are compatible with ART. Currently, Java version 7 release 76 (32 bit) is the only version of Java that is recommended by Mediware in order to run ART. If you need to download the correct version of Java, open a ticket with NH HMIS. Earlier versions of Java are not recommended due to other issues with Java itself that make it unstable, but versions back to version 6 release 45 can be used, although they are not recommended. If newer versions of Java are installed on your system, we recommend that they be uninstalled, and Java version 7

release 76 (32 bit) be installed. We also recommend disabling the "automatic update" feature to prevent unwanted updates to an incompatible version.

- Monitor
  - Screen Display - 1024 x 768 (XGA)
- Processor
  - A Dual-Core processor is recommended. Avoid machines with single core processors, which are usually much older computers.
- Internet Connection
  - Broadband
- Browser
  - ServicePoint is designed to be compatible with the newest versions of Google Chrome, Mozilla Firefox, and Apple Safari
  - Browser Performance: In the context of ServicePoint 5, there are three factors that outweigh all others: data transfer efficiency, memory management, and machine speed.
    - Data Transfer - We have observed that transfer efficiency may quickly become an issue if the user's machine's internet connection or their browser has abnormalities. A very bad internet connection will have different effects in different browsers.
      - How to find out if you have data transfer problems:
        - If things are fast, you don't have data transfer problems. If pages seem to load slowly or not at all, you may have data transfer problems; or you may have browser problems. At this point, a transfer problem is not certain, but may be possible.
    - Memory Management - Some browsers handle memory differently than others. The best practice for determining the best browser is to see if you experience any of the following issues.
      - Effects of poor memory management:
        - Your overall system performance may degrade.
        - Your browser may suddenly seem to completely stop working. Blank pages may appear or certain page components won't work.
        - Your browser may run more and more slowly.
      - What to do:
        - If you suspect that you may have poor browser memory management, try updating your browser to a more recent version before switching to a different brand of browser. More than likely, any major issue will have been fixed with a more current release. If you still have issues, try switching to one of the other 3 major browsers. If you need help updating your browser, contact your IT Department.
    - Machine Speed - Avoid machines with single core processors, which are usually much older computers. If your computer is a single-core machine operating at less than 2 GHZ, and you are not content with its performance:
      - Switch to one of the fastest browsers. Chrome is recommended, Firefox is a good alternate; Internet Explorer versions 8, 9 and 10 are acceptable (see below for information regarding Internet Explorer version 11).

- Run no unnecessary programs while using ServicePoint.
- Monitor your CPU usage in Task Manager. If it is frequently at 100%, you need a more capable machine.
- Think about getting more RAM. But before you buy enough RAM to max out your computer, consider replacing your old computer with a new or used dual-core machine. Even an old dual core tends to outperform a fully-upgraded, single-core in ServicePoint 5. Buying a used computer may actually cost less than buying a gigabyte or two of obsolete RAM for an older machine.

Note: Mediware is working on a new version 6; it is expected to be a replacement reporting too that will not require JAVA. Release date TBD.

- ART Users
  - The Advanced Reporting Tool (ART) only supports Java 7 release 7 (32 bit). Any higher versions of Java are not currently supported. We do not recommend the 64-bit version of Java because Chrome is a 32 bit only browser and the 64-bit version of Java does not function in Chrome.

**Internet Connectivity**
Participating Program must have Internet connectivity for each workstation accessing the HMIS. To optimize performance, all agencies are encouraged to secure a high speed Internet connection with a cable modem, DSL, FiOS, or T1 line.

**Security Hardware/Software**
All workstations accessing the HMIS need to be protected by a Firewall. If the workstations are part of an Agency computer network, the Firewall may be installed at a point between the network and the Internet or other systems rather than at each workstation. Each workstation also needs to have anti-virus and anti-spyware programs in use and properly maintained with automatic installation of all critical software updates. Good examples of anti-virus software include McAfee and Symantec (Norton) Security systems, among others.

**Agency Workstation Access Control**
Access to the HMIS will be allowed only from computers specifically identified by the Participating Agency's Executive Director or authorized designee and HMIS Agency Administrator. Laptop computers will require an additional security statement indicating that they will not be used for unauthorized purposes from unauthorized locations. Access to these workstations will be controlled through both physical security measures and a password. Each Agency's HMIS Agency Administrator will determine the physical access controls appropriate for their organizational setting based on HMIS security policies, standards and guidelines. Each workstation, including laptops used off-site, should have appropriate and current firewall, and virus protection as specified above, see *Security Hardware/Software section.* Devices must only access secured, password- protected Wi-Fi with non-public access.

## A.17. TECHNICAL SUPPORT/ASSISTANCE

**Policy**
The City of Waco will provide technical assistance including ongoing software support for users of the HoT HMIS. Internal hardware and internet connectivity issues should be addressed by the Partner's internal IT

staff. Even though the equipment and internet connection used to connect to the HoT HMIS is owned by the Partner, the City of Waco will provide technical assistance when possible and as resources allow.

**Procedure**
Hardware and connectivity issues not related to the HMIS software should be addressed by the Partner's internal IT staff. Partners may contact the HoT HMIS Administrator for technical support of the components necessary to connect to the HoT HMIS.

**Technical Assistance Request from Participating Agency**
End user contacts Agency Administrator with question or concern.
Agency Administrator Staff attempts to resolve issue. If unable to resolve, agency staff will contact the HMIS Administrator via electronic Technical Assistance Request (available on THE HOTHC website). If the issue is of an urgent nature HMIS staff can be contacted directly in order to request expedited service. Receipt of all requests will be sent within one business day and resolved as quickly as possible.
HMIS Administrator determines resources needed for service and if necessary, contacts software vendor for support.

**Chain of communication**
(Problems should be resolved at the lowest possible level to assure minimum time to resolution).

- End User
- Agency Administrator
- HMIS Administrator

### A.18. TRAINING MANUAL

**Policy**
A HoT HMIS Training Manual will be given to each new user upon initial training along with The Heart of Texas HMIS Policy and Standard Operating Procedures Manual. Technical assistance is offered throughout the duration of a user's employment with a Partner. The HoT HMIS Training Manual will provide specific technical instruction to HoT HMIS Users about how to use ServicePoint. The manual will be revised and redistributed as significant updates are performed on *ServicePoint.*

**Procedure**
The HoT HMIS Administrator will create, distribute and update the HoT HMIS Training Manual. This will include procedures that are held in common for all Partners, as well as forms for customizing the Training Manual for each Partner.

### A.19. MONITORING AND EVALUATION

**Policy**
HoT HMIS Administrator will regularly monitor and evaluate the effectiveness of the HoT HMIS and, based on the information received, will continue to make enhancements to the HoT HMIS and the Policies and Standard Operating Procedures as necessary. This may include compliance with the HMIS Standard Operating Procedures and with HUD's Data and Technical Standards. Monitoring and evaluation helps ensure security and proper usage of the HoT HMIS.

**Procedure**

The HoT HMIS Administrator will conduct internal system monitoring and may contact Agency Administrators to schedule monitoring and evaluation visits. HoT HMIS Administrator's back up personnel of the City of Waco may also contact Agency Administrators or other Partner staff in relation to the HMIS portion of standard monitoring visits conducted by HoT HMIS Administrator over the course of each year.

Each quarter, the HMIS Administrator will generate Report Cards that include measurements of HMIS usage and CoC program performance criteria

1. Partner Agencies with failing HMIS grades will be required to attend refresher training.
2. CoC Agencies with consistent low performance or failing HMIS grades will be required to meet with the HMIS Administrator and Collaborative Applicant to discuss ways to improve data collection.
3. CoC Agencies with consistent failing grades will be required to document an improvement plan.
4. CoC Agencies unable to improve HMIS usage and performance may have funds reallocated based upon a recommendation from the Independent Evaluation Committee and approval by the CoC Committee.

# B. Security and Access

## B.1. USER ACCESS

**Policy**

The HoT HMIS Administrator will provide unique user names and initial passwords to each Partner user. User names will be unique for each user and will not be exchanged or shared with other users. The HoT HMIS Administrator will have access to the list of user names for the HoT HMIS and will track user name distribution and use. Only the City of Waco will be authorized to purchase or grant additional user licenses to an Agency that has utilized all current licenses. Unique user names and passwords are the most basic building block of data security. Not only is each user name assigned a specific access level, but in order to provide to clients or program management an accurate record of who has altered a client record, when it was altered, and what the changes were it is necessary to log a user name with every change. Exchanging or sharing user names seriously compromises the security of the HoT HMIS, and will be considered a breach of the user agreement and will trigger appropriate repercussions and/or sanctions for the user and agency.

**Procedure**

The HoT HMIS Administrator will provide unique user names and initial passwords to each user upon completion of training, signing of a confidentiality agreement and receipt of the Policies and Standard Operating Procedures Manual. The sharing of user names will be considered a breach of the user agreement. The HoT HMIS Administrator is responsible for distributing user names and initial passwords to agency users and can also provide current users with a new password if he/she requires one.

## B.2. USER CHANGES

**Policy**

The HoT HMIS Administrator will make any necessary changes to the Partner user accounts. This includes issuance of new passwords and managing access levels, etc. The Agency Administrator is required to contact the HoT HMIS Administrator immediately upon a change in status of any user within their Partner Agency. Upon receipt of this change in status the HoT HMIS Administrator will take action to produce the needed changes in access for the specified user if the Agency Administrator has not already done so. The HoT HMIS Administrator has the ability to change user names and redistribute user licenses to accommodate the Partner organization.

**Procedure**

The HoT HMIS Administrator will make any necessary changes to the list of Partner users. Changes in Agency Administrators must be reported to the HoT HMIS Administrator. The Agency Administrator is required to notify the HoT HMIS Administrator of a terminated employee immediately upon termination of employment. For employees with user access otherwise leaving the agency, the user license should be revoked at the end of business on the person's last day of employment.

## B.3. PASSWORDS

**Policy**

Users will have access to the HoT HMIS via a user name and password. Passwords must be changed a minimum of once every 45 days. Users will keep their passwords confidential. Under no circumstances shall a

licensed user share a password nor shall they post their password in an unsecured location. These methods of access are unique to each user and are confidential. Users are responsible for keeping their passwords confidential. For security reasons, passwords will automatically be reset every 45 days.

**Procedure**
The HoT HMIS Administrator will issue a user name and temporary password to each new user who has completed training. Upon sign in with the user name and temporary password, the user will be required by the software to select a unique password that will be known only to that specified user. Every 45 days, passwords are reset automatically by the HoT HMIS software.

### B.4. PASSWORD RECOVERY

**Policy**
The HoT HMIS Administrator will reset a user's password in the event the password is lost or forgotten. Agency Administrators also have the capability to reset a user's password. Either Administrator must validate the authenticity of the request if the request is not made in person.

**Procedure**
In the event of a lost or forgotten password, the user whose password is lost will contact the Agency Administrator or the HoT HMIS Administrator. The Administrator will reset the user password, and issue a temporary password to allow the user to login and choose a new password. The new password will be valid from that time forward, until the next 45-day forced change. Administrators must validate the authenticity of the request if the request is not made in person. In other words, neither Agency Administrators nor the HoT HMIS Administrator shall issue a new password without ensuring that the person requesting it is, in fact, the person with the authorization to use it. For example, if a request is made by phone or email, the Agency Administrator or System Administrator should call the user back at his/her desk (using the contact number on file) before issuing a new password.

### B.5. EXTRACTED DATA

**Policy**
HoT HMIS users will maintain the security of any client data extracted from the database and stored locally, including all data used in custom reporting. HoT HMIS users will not electronically transmit any unencrypted client data across a public network. The custom report-writer function of ServicePoint allows client data to be downloaded to an encrypted file on the local computer. Once that file is unencrypted by the user, confidential client data is left vulnerable on the local computer, unless additional measures are taken. Such measures include restricting access to the file by adding password protection. For security reasons, unencrypted data may not be sent over a network that is open to the public. Unencrypted data may not be sent via email. HMIS users should apply the same standards of security to local files containing client data as to the HMIS database itself.

**Procedure**
Data extracted from the database and stored locally will be stored in a secure location (not on floppy disks/CDs or other temporary storage mechanisms like flash drives or on unprotected laptop computers, for example) and will not be transmitted outside of the private local area network unless it is properly protected via encryption or by adding a file-level password. The HoT HMIS Administrator will provide help in determining

the appropriate handling of electronic files. All security questions will be addressed to the HoT HMIS Administrator. Breach of this security policy will be considered a violation of the user agreement, which may result in personnel action and/or agency sanctions.

### B.6. DATA ACCESS COMPUTER REQUIREMENTS

**Policy**

Users will ensure the confidentiality of client data, following all security policies in the HoT HMIS Policies and Standard Operating Procedures Manual and adhering to the standards of ethical data use, regardless of the location of the connecting computer. All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer. HMIS Administrator may restrict access to the HoT HMIS to specific computers in the future. Because ServicePoint is web-enabled software users could conceivably connect to the database from locations other than the Partner itself, using computers other than agency-owned computers. Connecting from a non-agency location may introduce additional threats to data security, such as the ability for non-*ServicePoint* users to view client data on the computer screen or the introduction of a virus. If such a connection is made, the highest levels of security must be applied, and client confidentiality must still be maintained. This includes only accessing the HoT HMIS via a computer that has virus protection software installed and updated.

**Procedure**

Each Partner and Agency Administrator is responsible for:

1. Physical Space. Partners must take reasonable steps to ensure client confidentiality when licensed users are accessing the HoT HMIS. Licensed users are required to conduct data entry in a protected physical space to prevent unauthorized access to the computer monitor while confidential client information is accessible.

2. Use of a non-agency computer located in a public space (i.e. Internet café, public library) to connect to HMIS is prohibited.

3. Time-Out Routines. Each Agency Administrator will be required to enable time-out (login/logout) routines on every computer to shut down access to the HoT HMIS when a computer is unattended. Time-out routines will be engaged at a minimum after 10 minutes of inactivity or at other intervals as determined.

4. Each computer that accesses HMIS must have current virus software that updates automatically installed.

5. If the HMIS is accessed over a network, the network must be protected by a hardware or software firewall at the server. A stand-alone machine that accesses HMIS must also have a hardware or software firewall installed and active. This may be the firewall protection included as part of the operating system or the virus protection software installed on the computer.

*Questions about security of the HoT HMIS should be referred to the HoT HMIS Administrator.*

# C. Agency Participation Requirements

## C.1. HOT HMIS AGENCY AGREEMENTS

**Policy**

Only Partners will be granted licenses to access the HoT HMIS system. The City of Waco shall make the sole determination to identify Partners. The Executive Director (or appropriate designee) will be required to sign the "HMIS Partner Agreement" (Attachment A) binding their organization to the HoT HMIS Policies and Standard Operating Procedures and all applicable laws and regulations regarding the handling of client data before access is granted. The City of Waco has final authority over the HoT HMIS. In order to ensure the integrity and security of sensitive data, City of Waco will regulate access to this data. Only Agencies that have agreed to the terms set out in the HMIS Agency Agreement will be allowed access to the HoT HMIS. The agency agreements will include terms of access, an acknowledgement of receipt of the Policies and Standard Operating Procedures Manual, and an agreement to abide by all provisions contained therein.

Participating Agencies shall sign a Memorandum of Understanding and comply with the stated requirements. Agencies will be granted access to the HMIS software system after:

- The MOU has been signed with the City of Waco, and
- Agencies put into place the stated requirements in the MOU.

**Procedure**

Partners will be given a copy of the HMIS Agency Agreement, the Policies and Standard Operating Procedures Manual, and any other relevant paperwork in time for adequate review and signature. Once that paperwork has been reviewed and signed by the Executive Director (or appropriate designee), the HoT HMIS Administrator will issue a certain number of licenses for use by the agency and assist with the set-up of an Agency Administrator. Agency users will be trained to use ServicePoint by the HoT HMIS Administrator. Once training has been completed, each user will be issued a user name and password by HOT HMIS Administrator.

Agencies agree to comply with these policies and procedures.

## C.2. USER LICENSES

**Policy**

In order to obtain a license, a user must successfully complete training by the HoT HMIS Administrator and must sign a User License Agreement (Attachment B) upon completing training. Sharing of licenses, User IDs or passwords is strictly prohibited. If necessary, Partners may purchase additional User Licenses from Mediware Information Systems, Inc. through the City of Waco. The cost for User Licenses will be determined by the City of Waco based on Mediware charges and funding availability. The City of Waco purchases a number of user licenses on behalf of the HoT HMIS and determines the number of users appropriate for participating agencies. Partners may need to purchase additional User Licenses. This purchase can be made at any time.

**Procedure**

Each Agency Administrator (or Executive Director) will identify the staff designated to be the licensed users of the HoT HMIS and submit the names to the HoT HMIS Administrator. The City of Waco determines the number of users appropriate for participating agencies based on the list provided and other factors. Partners wishing to purchase additional User Licenses will notify the HoT HMIS Administrator. The HoT HMIS Administrator will purchase the User Licenses from Mediware Information Systems, Inc. and bill the Partner accordingly. The HoT HMIS Administrator purchases licenses online, through the ServicePoint program. The HoT HMIS Administrator will then notify the Partner when the additional Licenses are available. Mediware invoices The City of Waco for the cost of the licenses. Then, in turn, the City of Waco invoices the responsible Agency accordingly.

### C.3. USER ACTIVATION

**Policy**

Each new user will be issued a user name and password to access the HoT HMIS upon approval by the Agency Administrator or System Administrator, completion of ServicePoint training and signing of the HMIS User Agreement. Every user must receive appropriate ServicePoint training before being issued a user name and password.

**Procedure**

The HoT HMIS Administrator will distribute user licenses for Partners. Agency Administrators are responsible for notifying the HoT HMIS Administrator of user changes. The HoT HMIS Administrator will be responsible for training all new users. The HoT HMIS Administrator will provide training to Agency Administrators and all users in the Partner Agency and will supplement this training as necessary.

### C.4. HMIS USER AGREEMENTS

**Policy**

Each Partner User will sign the HoT HMIS User Agreement before being granted access to the HoT HMIS. Clients' confidential information is not to be accessed or shared for any reason other than job performance. User names and passwords are not to be shared under any circumstances. Any breach in this contract will result in immediate action. Before being granted access to the HoT HMIS, each user must sign an HMIS User Agreement, stating that he or she has received or is in the process of training, will abide by the HoT HMIS Policies and Standard Operating Procedures Manual, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in the HoT HMIS relevant to the delivery of services to people in housing crisis in the Heart of Texas.

**Procedure**

The Agency Administrator or HoT HMIS Administrator will distribute HMIS User Agreements to new HMIS Users for signature. The HoT HMIS Administrator will file signed HMIS User Agreements for all users. Allowing a user access to the HoT HMIS without a signed user agreement is a violation of the HoT HMIS Policy & Standard Operating Procedures and may result in program sanctions.

## C.5. TRAINING

**Policy**

The HMIS Administrator is responsible for defining training needs and organizing training sessions for system users. The HoT HMIS Administrator will provide various training options, to the extent possible, based on the needs of HMIS users. The HoT HMIS Administrator will provide for adequate and timely *ServicePoint* training. The training schedule may be obtained from the HoT HMIS Administrator. In order for the HoT HMIS to be a benefit to clients, a tool for Authorized Agencies and a guide for planners, all users must be adequately trained to collect, enter and extract data.

The agency admin is also responsible for making sure the proper training has occurred for the users in their agency and that HMIS policies are being followed. Agency admins must also notify the HMIS administrator if any changes have occurred to their program.

**Procedure**

The HMIS Administrator will provide access to training for all HMIS users. Agency Administrators will be given additional training relevant to their position.

Each end user will be required to attend a refresher each year. Each Agency Admin will be required to attend an Agency Admin training and a report training each year.

**New User/Referesher Training:** (Offered Quarterly)
New User Training is designed for staff members who will need to start using ServicePoint. This training is required of all new ServicePoint users before access to the protected ServicePoint website. This training will cover history, importance of data, ethics, and basic ServicePoint overview.

**Agency Admin Training:** (Offered Bi-Annual)
Agency admin training is required of all current or new ServicePoint users who are stepping up into the role of Agency Admin. The agency admin at each agency is our point of contact at each agency in regards to ServicePoint and is required to submit certain reports to our HMIS team each month, train new users in agency specific ServicePoint workflow, and attend HMIS Advisory meetings. The Agency Admin must go through a New User training prior to completing the Agency Admin training.

**Reporting Tool:**
Training dates will be added as necessary when a new Agency Admin comes on board or someone gets a reporting license.

## C.6. CONTRACT TERMINATION INITIATED BY PARTNER

**Policy**

Partners may terminate the HMIS Agency Agreement with or without cause upon 30 days written notice to the City of Waco and according to the terms specified in the HMIS Agency Agreement. The termination of the HMIS Agency Agreement by the Partner may affect contracts issued by HUD. In the event of termination of the HMIS Agency Agreement, all data entered into the HoT HMIS will remain an active part of the HoT HMIS. While Partners may terminate relationships with the HoT HMIS, the data entered prior to that termination

would remain part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in the Heart of Texas.

**Procedure**

Certain Provider Agencies are required to participate in the HoT HMIS as a condition of their funding. For all non-HUD Funded Partners terminating the HMIS Agency Agreement, the person signing the HMIS Agency Agreement (or a person in the same position within the agency) will notify HMIS Administrator 30 days or more from the date of termination. In all cases of termination of HMIS Agency Agreements, the HoT HMIS Administrator will inactivate all users from that Partner on the date of termination of agreement.

### C.7. CONTRACT TERMINATION INITIATED BY THE CITY OF WACO

**Policy**

On behalf of the City of Waco the HoT HMIS Administrator may terminate the HMIS Agency Agreement for non-compliance with the terms of the agreement or with the HMIS Policies and Standard Operating Procedures with written notice to the Partner. The HMIS Administrator may also terminate the HMIS Agency Agreement with or without cause with 15 days written notice to the Partner and according to the terms specified in the HMIS Agency Agreement. If a Partner's contract is terminated under the terms of that contract, the agreement for HMIS access for that program will also be terminated. In that case, access will be renegotiated by the HoT HMIS Administrator and the agency in accordance with these standard operating procedures. The termination of the HMIS Agency Agreement may affect contractual relationships with HUD. In the event of termination of the HMIS Agency Agreement, all data entered into the HoT HMIS will remain a part of the HoT HMIS. If termination of the HMIS Agency Agreement occurs, all Partner users will be inactivated on the date the HMIS Agency Agreement or contract is terminated. While the HMIS Administrator may terminate the HMIS Agency Agreement with the Partner, the data entered by that Partner prior to termination of contract would remain part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in the Heart of Texas.

**Procedure**

When terminating the HMIS Agency Agreement, the HMIS Administrator of the City of Waco will notify the person from the Partner Agency who signed the HMIS Agency Agreement (or a person in the same or higher position within the agency) 15 days or more prior the date of termination of contract, unless the termination is due to non-compliance with the Standard Operating Procedures. Willful neglect or disregard of the Standard Operating Procedures may result in immediate termination of a Partner Agency from the HoT HMIS. In all cases of termination of HMIS Agency Agreements, the HoT HMIS Administrator will inactivate all users from that Partner Agency on the date of termination of contract.

# D.Data Collection, Quality Assurance, and Reporting

## D.1. REQUIRED DATA COLLECTION

**Policy**

Providers funded by HUD through the Supportive Housing Program, Shelter Plus Care, Section 8 Moderate Rehabilitation and the Emergency Shelter Grant are required to participate in HMIS by HUD. All Partners that participate in HMIS are considered "Covered Homeless Organizations" (CHO) and are required to comply with HUD's *HMIS Data and Technical Standards* unless those standards are in conflict with local laws.
This includes the collection of required data elements.

Providers shall attempt to collect basic information on every client served by the Provider upon intake into the Provider's facility or program. If client refuses or is unable to provide basic information, providers shall, at a minimum, enter each client as an Anonymous Entry into the HoT HMIS system. Partners may choose to collect more client information for their own case management and planning purposes.

**Assessment Data Collection**

Providers of certain programs shall attempt to conduct detailed assessments on each client who has gone through the intake process and has been accepted into the Provider's facility or program. At a minimum, providers shall attempt to collect the assessment information required as part of HUD's Data and Technical Standards.

**Timeliness of Data Entry**

Providers are required to enter basic client intake data into the HoT HMIS weekly. All data entry must be completed on or before the following Monday for clients served during the prior week. Exceptions to these data collection policies are in place for domestic violence shelters. DV shelters by law are not allowed to participate in the HMIS. In order for the data contained within the HoT HMIS to beuseful for data analysis and reporting to funders, certain minimum data must be consistently collected throughout the system.

**Client entry and exit dates**

It is important for users to accurately capture entry and exit dates for clients in their programs. If data is being entered after the client'sactual entry, the user needs to be sure that the date stamp on the Entry/Exit for that client accurately portrays the entry for that program. When making changes to client's profiles, a user should do so through the client's Entry/Exit tab. If a client is stayingin a shelter program, updates and changes should be done through the ShelterPoint Entry/Exit for that client. If an incorrect Exit Date is entered, the user must delete the Entry/Exit for that client as well as any services associated with it and enter the data again.

**Procedure**

Each agency should review Attachment E to determine the type of data that is required to be collected and entered into HMIS.

### D.2. CLIENT CONSENT

**Policy**

Each agency must post a sign at each intake or comparable location explaining the reasons for data collection for those seeking services. Consent for entering of data into HMIS is to be documented by the ROI when the client accepts the services offered. The client has the option to opt out of allowing his or her identifying information to be added to the database. In that case, the client's data should be added to the HoT HMIS without identifiers although the record should be tracked internally by the agency to minimize the number of duplicate records for one client. Electronic client data will be shared among Partners. Privacy Policies should be in effect for each agency to both inform clients about the uses and disclosures of their personal data and to protect the agency by establishing standard practices for the use and disclosure of data. Client consent notices must contain enough detail so that the client may make an informed decision.

**Procedure**

HMIS has an established privacy policy which will be posted in appropriate areas for client review at each Partner Agency (Attachment D). The HMIS Administrator will review the privacy notices as part of the annual HMIS review and/or through regular monitoring. If a client denies permission to enter confidential data, the Partner will enter the de-identified data into the HoT HMIS and track the record to minimize duplicate records for each client.

### D.3. RELEASE OF INFORMATION

**Policy**

The Heart of Texas HMIS operates as an open data sharing system. This means that the client data collected by Partners is shared information. This is most effectively achieved when the Release of Information (ROI) is established in the system for each client served and by each Provider. The ROI must begin on the day (or a date prior to) the data is entered into the HMIS. The ROI is to remain effective for a time period of three years. During this three year span of time, the client's data is viewable by all Partners in the HoT HMIS. Aggregate data may be released to the public for purposes beyond those specified in HUD HMIS Data Standards Manual. All publicly released data must be anonymous by removal of all identifiers and/or all information that could be used to infer an individual or household identity.

**Procedure**

Each client served is required to read and sign a ROI. The ROI will then be established on or before the date of data entry in order for the client data to be shared properly with other Partners.

### D.4. APPROPRIATE DATA COLLECTION

**Policy**

HoT HMIS users will only collect client data relevant to the delivery of services to people in housing crises in the Heart of Texas and/or required by funders or by law. The purpose of the HoT HMIS is to support the delivery of homeless and housing services in the Heart of Texas. The database should not be used to collect or track information not related to serving people in housing crises or otherwise required for policy development and planning purposes.

**Procedure**

Agency Administrators will ask the HoT HMIS Administrator for any necessary clarification of appropriate data collection. The HoT HMIS Administrator, in consultation with the City of Waco, will make decisions about the appropriateness of data being entered into the database. This concern targets data elements that can be consistently tracked and reported, and does not specifically target the contents of case management notes or other fields not to be aggregated.

### D.5. DATA OWNERSHIP

**Policy**

The HoT HMIS, and any and all data stored in the HoT HMIS, is the property of the City of Waco. The City of Waco has authority over the creation, maintenance and security of the HoT HMIS. Violations of the HoT HMIS Agency Agreement, the HoT HMIS Policies and Standard Operating Procedures, privacy policies developed at the agency level, or other applicable laws may subject the Partner to discipline and/or termination of access to the HoT HMIS. In order to ensure the integrity and security of sensitive client information and other data maintained in the database, the City of Waco will be responsible for data ownership.

**Procedure**

The HMIS Agency Agreement includes terms regarding the maintenance of the confidentiality of client information, provisions regarding the duration of access, an acknowledgement of receipt of the Policies and Standard Operating Procedures Handbook, and an agreement to abide by all policies and procedures related to the HoT HMIS including all security provisions contained therein. Because programs participating in the HoT HMIS are funded through different streams with different requirements, the City of Waco shall maintain ownership of the database in its entirety in order that these funders cannot access data to which they are not legally entitled.

### D.6. DATA ENTRY: PROFILE INFORMATION

**Policy**

Users will designate profile information as open in the client security portion of the profile section of a client record in ClientPoint except in extreme cases. No user will close the profile section of a client record. Some users (depending on the level of access) have the ability to determine whether information in client records is “open” or “closed” to users from other Agencies. Open sections of the record can be seen and changed by users from another agency; closed sections of the record cannot be seen by users from another agency. Because the HoT HMIS is an open system, the default setting on client records has been set to “open.”

**Procedure**

Users will designate all client records as open. Only in extreme circumstances will the record of a client be closed. For example, personal medical or legal history that has been entered into the system; only this section of the client’s data is set to closed.

### D.7. DATA ENTRY: ASSESSMENT CUSTOMIZATION

**Policy**

Partners may have fields available for agency-specific assessment customization. ServicePoint may include fields that can be customized on the Partner level to reflect the program-specific data collection needs of its programs. These fields are part of the ServicePoint program and are available at no additional cost. Agency

Administrators will have the ability to customize these fields. Because these fields may be customized at the Partner level, Agency Administrators have the ability to add, delete and change custom fields and do not need the assistance of the HoT HMIS Administrator to perform these customizations.

**Procedure**
Agency Administrators can be trained to customize the agency-specific fields. However, the HMIS Administrator is available to perform these duties as needed.

### D.8. DATA INTEGRITY

**Policy**
HoT HMIS users will be responsible for the accuracy of their data entry. The Agency Administrator will be responsible for ensuring that data entry by users is being conducted in a timely manner and will also ensure the accuracy of the data entered. The quality of HoT HMIS data is dependent on individual users to take responsibility for the accuracy and quality of their own data entry. Agency Executive Directors and/or Agency Administrators are responsible for monitoring the quality of the data for their own program(s), since that data may be used for reporting and/or monitoring purposes. Data may also be used to measure program efficacy, which impacts funding opportunities during competitive funding processes such as the annual Continuum of Care application to HUD.

**Procedure**
In order to test the integrity of the data contained in the HoT HMIS, the HoT HMIS Administrator will perform regular data quality checks on the HoT HMIS. The data quality checks will include reporting of "overlaps," periodic verification of data and comparison to hard files, as well as querying for internal data consistency and null values. Any patterns of error will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to make corrections where possible, correct data entry techniques, improve the accuracy of their data entry, and will be monitored for compliance. Reports will be assessed for data quality and errors will be reported to the Agency Administrator. Other reports for non-HUD funded programs may also be required. The HoT HMIS Administrator reserves the right to add reporting requirements if data quality appears to be decreasing or if reporting requirements change.

### D.9. QUALITY CONTROL: DATA INTEGRITY EXPECTATIONS

**Policy**
Accurate and consistent data entry is essential to ensuring the usefulness of the HoT HMIS. Partners will provide acceptable levels of timeliness and accuracy. Data quality is an important aspect of the HoT HMIS, and must be maintained at the agency level and by users of the system. The HMIS Administrator will monitor data quality as part of the HMIS management functions.

**Procedure**
The HoT HMIS Administrator will perform regular data integrity checks on the HoT HMIS.

### D.10. CLIENT DATA RETRIEVAL

**Policy**
Any client may request to view, or obtain a printed copy of, his or her own records contained in the HoT HMIS. The client will also have access to a logged audit trail of changes to those records. No client shall have access to

another client's records in the HoT HMIS. The data in the HoT HMIS is the personal information of the individual client. Each client has a right to know what information about him or her exists in the database, and to know who has added, changed or viewed this information, and when these events have occurred. This information should be made available to clients within a reasonable time frame of the request.

**Procedure**

A client may ask his/her case manager or other agency staff to see his or her own record. The case manager, or any available staff person with HoT HMIS access, will verify the client's identity and print all requested information. The case manager can also request a logged audit trail of the client's record from the Agency Administrator. The Agency Administrator will print this audit trail; give it to the case manager, who will give it to the client. The client may request changes to the record, although the agency can follow applicable law regarding whether to change information based on the client's request. A log of all such requests and their outcomes should be kept on file in the client's record.

### D.11. PUBLIC DATA RETRIEVAL/REQUESTS FOR DATA

**Policy**

The HMIS Administrator will address all requests for data from entities other than Partners or clients. No individual client data will be provided to any group or individual that is neither the Partner that entered the data or the client him or herself without proper authorization or consent. The HMIS Administrator will provide aggregate reports for the larger community. The content of these reports will reflect a commitment to client confidentiality and ethical data use. Any requests for reports or information from an individual or group who has not been explicitly granted access to the HoT HMIS will be directed to the HMIS Administrator. No individual client data will be provided to meet these requests without proper authorization or consent.

**Procedure**

All requests for data from anyone other than a Partner or a client will be directed to the HMIS Administrator or her designee. As part of the mission to end homelessness in the Heart of Texas, it is the HMIS Administrator's policy to provide aggregate data on homelessness and housing issues in this area. No individually identifiable client data will be reported in any documents.

### D.12. DATA RETRIEVAL SUPPORT

**Policy**

Partners will create and run agency-level reports. The Agency Administrator has the ability to create and execute reports on agency-wide data. This allows Partners to customize reports and use them to support agency-level goals. The HoT HMIS is to be a tool for the Partners in managing programs and services.

**Procedure**

The Agency Administrator will be trained in the use of reporting tools by the HMIS Administrator. The HoT HMIS Administrator may assist Agency Administrators with the development of reports/queries for their specific use.

# E. Other HMIS Information

## E.1. HoT HMIS Security Infrastructure

The following information about how HoT HMIS data is protected from unauthorized access or use is provided here for the benefit of all Partners, public officials, advocates and consumers who are interested in the architecture of security.

**Server Hosting at Mediware's Location**
The City of Waco has co-located the HoT HMIS database and web application servers in Shreveport, Louisiana, at the headquarters of Mediware Information Systems, Inc. This is done to take advantage of Mediware's ability to provide 24-hour security and support for HoT HMIS hardware and software. Co-location means that while City of Waco owns the hardware and software, it pays a monthly maintenance fee for Mediware to provide both server hosting and routine server maintenance.

Mediware employs a full time staff of experts dedicated to keeping their clients up and running, secure, and using the latest technology. This technology includes physical security, Cisco firewalls, authentication through Verisign certificates, Windows' secure server technology, and 128-bit encryption of usernames, passwords and all data passing to and from the database. It is the job of the HoT HMIS Administrator and back up personnel to maintain a point of contact between Mediware and City of Waco and keep track of any security issues related to the hosting of the HoT HMIS database.

**Physical Attack**
The database server and web server are located in a physically secure building where security guards are employed to monitor security from 7:00 a.m. to 7:00 p.m. Monday through Friday, and from 8:00 a.m. to 4:00 p.m. on Saturdays. During off hours, a card key is required to enter the building. Within the building, the Mediware offices are also locked with a separate key structure. The server itself deploys the standard security measures to prevent unauthorized local access.

**Network Attack**
Mediware uses Cisco firewalls to prevent unauthorized remote access to the database server. A firewall is a software application that blocks all incoming electronic traffic except traffic that is explicitly permitted. Permissions are configured manually by network administrators. This combination of firewalls and virus protection software will detect and prevent most viruses, Trojan horses, worms, malicious mobile codes or email bombs from damaging our database.

**Denial of Service**
The combination of firewalls and routine monitoring of network traffic by skilled professionals (Mediware network administrators) will detect and prevent an attacker from flooding our server to the point of failure.

**Exploitation of Operating System Vulnerabilities**
As part of the maintenance contract, network administrators at Mediware are responsible for updating the server with the latest software patches and fixes of known operating system weaknesses. Keeping abreast of software patches and reports of new vulnerabilities is the best way to avoid falling prey to these attacks.

**Exploitation of Software Vulnerabilities**
Because the City of Waco relies on the same company who created the ServicePoint software to host its server, City of Waco is assured that security holes discovered in the ServicePoint software will be addressed by technicians with access to timely and accurate information about the core program. City of Waco does not need to rely on second- or third-hand software alerts or the installation of patches and upgrades by network administrators unfamiliar with the product. This is a great advantage in combating application-specific security issues.

**User Falsification**
Using a public-key infrastructure and signed digital certificates, the latest security technology available, Verisign provides a safe and reliable method of authenticating users. These methods, while they do employ traditional user names and passwords at their base, also encrypt data and provide a software-enabled check and counter-check methodology that make stealing identities or masquerading as an authorized user virtually impossible. In addition, these methods produce one-time use session keys that foil a replay attack, as user credentials will never be signed and encrypted in precisely the same way twice.

**Data Traps**
Verisign provides 128-bit SSL encryption of all data passing from agency to server, or server to agency. Encryption is the translation of data from a readable “clear text” to an encoded hash using complex mathematical algorithms. SSL, short for secure sockets layer, is a data transport protocol that encrypts data using a public-key infrastructure. It is estimated that data encrypted with 128-bit encryption would take at least a trillion years to crack using today’s technology. When data is encrypted, even if packets could be captured or recorded as they travel across the Internet, they could not be decoded and read.

**Server Falsification**
The public-key infrastructure provided by Verisign provides not only authentication of the agency, but also authentication of the web site, and hence, authentication of the hosting server. Authentication is provided through digital certificates verified by Verisign, and is an integral part of the login process. Mutual authentication prevents a rogue web site from masquerading as our secure web site and drawing sensitive data.

**Social Engineering**
These are attacks in which a social situation (for example, a customer service call from a third-party company) is manipulated so that an unauthorized user gains access to protected information, such as client data, or user names and passwords. The biggest deterrent to social engineering is clear policies and procedures. It is much harder for users to be manipulated into providing confidential information if they have clear and thoughtful rules to follow when providing such information. City of Waco provides clear policies and procedures around issues of ServicePoint data confidentiality and confidentiality of user names and passwords. These policies and

procedures are designed to speed problem resolution and minimize the chance of a user being manipulated into divulging confidential data through confusion or a sincere desire to help someone in need.

**Misuse of Privileges**

ServicePoint provides several levels of user access to the database. Each level has access to a particular subset of information and particular abilities to manipulate information. City of Waco provides clear "job descriptions" for each level of access, to ensure that each user is assigned an appropriate level of access. The City of Waco provides clear protocol and procedures for handling data needs and requests that fall outside of a particular user's job description. Finally, City of Waco will provide clear procedures for handling changes in access levels and users, as well as for password recovery and other access issues. These procedures will be designed to clarify and streamline the daily work of legitimate users, and minimize the chance of legitimate users misusing privileges even towards legitimate ends.

**Local Physical Attack**

Agency computers are necessarily more physically vulnerable than our central server. As no ServicePoint data is stored on the local computer the physical vulnerability of these computers does not constitute a significant threat to client confidentiality regarding this data. However, any user access data, such as a password, that is stored on a computer or in a written file, does constitute a risk to client confidentiality. Even if a computer or server are stolen, (one key), the data is still safe and remains unreadable.

*The guidelines set forth in this document are subject to change.*

# HEART OF TEXAS
# HOMELESS MANAGEMENT INFORMATION SYSTEM
# POLICIES AND STANDARD OPERATING PROCEDURES
# ATTACHMENT A

# PARTNER PARTICIPATION AGREEMENT

## *Heart of Texas*

## *Homeless Management Information System*

**HoT HMIS:**

The Heart of Texas Homeless Management Information System (Hot HMIS) is a network of organizations committed to improving service access and the development of services to address the unmet needs of residents living in the Heart of Texas Region. HoT HMIS utilizes a client database that allows for the tracking of clients to determine the services a client has already received and services the client needs that may be lacking in our community. The HoT HMIS provides the ability to track homeless individuals in the community as well as their progress. The goal of the HoT HMIS is to have all organizations that provide services to homeless and low income individuals and their families identified in its database, and to have as many of these service providers as possible utilizing the system.

The HoT HMIS was created to improve the delivery of services to individuals who have unmet needs. The system is designed to allow for referrals, evaluating service needs, case management, client tracking, management of homeless information, creating reports and regional analysis of service delivery. Information in the HoT HMIS should be used ONLY for the above stated purposes. Any other use of this information is prohibited. Agencies should communicate to users the importance of maintaining the confidentiality of client data in the HoT HMIS.

The HoT HMIS uses the ServicePoint software, which is a product of Mediware Information Systems, Inc. The ServicePoint software is an Internet-based application providing real-time access. All that is needed to log into the system is Internet access, a web browser, a user ID and password. Real-time access provides immediate update of information entered into the system.

For an agency to be a HoT HMIS Partner, an administrator of that agency/organization must sign this Partner Participation Agreement form detailing the specific expectations of the partner organizations. All users of the HoT HMIS will be required to complete and sign a User Confidentiality Agreement.

As a HoT HMIS Partner, agencies have certain obligations and requirements that must be followed in order to protect the rights and interests of HoT HMIS clients. Below are performance standards required of each agency and its employees who use the HoT HMIS. It is the agency's responsibility to ensure that each user is familiar with the requirements of the system.

**Client Rights:**

In order for information to be shared in the HoT HMIS, the client or his/her legal guardian must give consent to release their information to participating HoT HMIS Partners. The client has the right to refuse to release his/her information. If the client refuses to do so, this in no way affects the client's eligibility for services at any agency. Refusal to give consent to release information requires that you enter client information and mark it as RESTRICTED in the system, so that no one, other than your agency and the system administrator(s), can access this information.

Client information may be used only for purposes specified by the client. Client information may not be shared for purposes other than those related to a user's job duties. Such unauthorized use is prohibited and will result in termination of access to the system by a majority vote of the HoT HMIS Advisory Committee.

**User Accounts:**

Each user of the HoT HMIS will be assigned a user ID and password. The user may ***not*** share the ID and password with anyone. This will assure that only authorized persons are using the system. The user will be held accountable for all actions performed by the assigned ID. Each user is required to read and sign a User Confidentiality Agreement before he/she is given access to the system.

**Training:**

It is the responsibility of each Agency Administrator to ensure that each of its users is knowledgeable about the purpose of HoT HMIS, and knows how to correctly use the system.

Each agency is required to assign at least one person from their agency to be an Agency Administrator who will serve as a contact with the System Administrator of the HoT HMIS. This person will be required to attend training and is expected to obtain the knowledge necessary to train other users in that agency. This person will also relay problems and suggestions to the System Administrator of HoT HMIS.

**Data Integrity:**

The Partner Agency has the responsibility of ensuring the accuracy of the information entered into the system. The agency must be sure that its employees have been properly trained, made aware of the importance of recording accurate data and respect the confidentiality of clients in the system.

**Reporting and Analysis:**

One of the goals of the HoT HMIS is to track clients and the services they receive. This information can be used to determine what additional services are needed throughout the community. The information in the system will be used to produce reports about programs and services. As a HoT HMIS Partner, it is important that you record each and every potential client in the HoT HMIS so that HoT HMIS Administrators can track unmet needs as well as those that were met. This is crucial in order for us to perform an accurate analysis of community services and programs. The homeless providers that have been identified and trained to use the HoT HMIS should be aware that the system will be used to create reports on the homeless and the services that are provided to them. This aggregate data will be collected and used by the Heart of Texas Homeless Coalition to assist in determining the number of homeless persons in the community, among other statistics.

**Fees:**

As a member of HoT HMIS, each agency will be required to pay applicable fees. The City of Waco is providing the administration and maintenance of the HoT HMIS, including administration and maintenance of the databases, training, software support, negotiation of technology contracts and will serve as liaison to the HoT HMIS vendor. The annual fee is paid to the City of Waco in exchange for these services.

* Fees based on the following:
  $250 Activation Fee for every new license
  $150 License Fee for every Single Licensed Agency
  $150 License Fee for each license for Multiple Licensed Agency
  $90 ART License Fee annually per license

**Termination of Access:**

When participating agencies and/or users violate guidelines, HoT HMIS Administrator may terminate access to the system based on a majority vote of the HoT HMIS Advisory Committee.

An agency may choose to withdraw from the HoT HMIS with a written notice of desire to do so. An agency may choose to withdraw a user from the system for any reason deemed appropriate. In this case, it is required that the partner agency inform the HoT HMIS Administrator of the revocation of the particular user's access to the system.

**Agreement Effective Date:**

This agreement becomes effective on the date it is signed. Actual access to the system becomes effective once this Partner Participation Agreement and System User Confidentiality Agreement are signed, user names and passwords have been assigned and training has been completed. Once access to the system has been granted, it is effective for the term of the project, unless terminated for disciplinary actions or by written notice of a desire to withdraw from the HoT HMIS. Access to the system will be automatically renewed annually with submission of the agreed upon annual fee to HoT HMIS Administration.

This agreement and other HoT HMIS documents may be amended to comply with changes in state and federal legislation as needed.

**Agreement:**

As the Executive Director (or Designee) of _____, I have read, fully understand and agree to the terms and guidelines set forth in this Partner Participation Agreement form. I understand my responsibilities as a HOT HMIS Partner and further understand that failure to follow all guidelines set forth by HoT HMIS will result in the termination of my agency's access to HoT HMIS.

_____

Agency Name

_____ _____

Executive Director (or Designee) Signature Date

_____ _____

HoT HMIS Administrator Signature Date

# HOMELESS MANAGEMENT INFORMATION SYSTEM POLICIES AND STANDARD OPERATING PROCEDURES ATTACHMENT B

# *Heart of Texas HMIS*

# USER LICENSE CONFIDENTIALITY AGREEMENT

**Client Confidentiality:**

The Heart of Texas Homeless Management Information System (HoT HMIS) is a network of organizations committed to improving service access and the development of services to address the unmet needs of residents living in the Heart of Texas Region. As a representative of a HEART OF TEXAS HMIS partner organization, I understand I have access to confidential information, some of which is personal and is, by law, considered confidential. I will at all times treat this information as confidential, and will disclose this information only to explicitly authorized individuals and/or organizations for the purpose of service delivery. **I will not access or share confidential information for any reason other than to perform my job duties.**

**Initial:** _____

I understand that client confidentiality is of utmost importance; therefore, I agree to take the necessary measures to ensure that all client information is handled in strict confidence.

**Initial:** _____

**HEART OF TEXAS HMIS Access:**

I acknowledge that I will be assigned a user ID and password that is to be used **ONLY** by myself to access the HEART OF TEXAS HMIS. I understand that I will be held accountable for all actions and activities produced by my user ID. I will not share my ID and/or password with anyone, and I will not use the ID and/or password assigned to someone else.

**Initial:** _____

I will not enter any unauthorized data or change/alter existing data in a manner inconsistent with my job duties. Under no circumstances will I enter knowingly false data that may compromise the integrity of the system.

**Initial:** _____

I agree not to attempt to intentionally cause the system to malfunction or knowingly alter data without authorization in an effort to compromise the computer security system. I further agree to report any suspected misuse or lapse in the security system.

**Initial:** _____

**Statement of Understanding:**

By signing this agreement I acknowledge that I understand the purpose and intent of the HEART OF TEXAS HMIS, and understand the relationship of HEART OF TEXAS HMIS and the organization with which I am employed. I understand that maintaining client confidentiality is my first duty and largest responsibility as a user of the HEART OF TEXAS HMIS. I acknowledge that I have read, understand and voluntarily agree to follow the guidelines set forth above. I further understand that failure to follow these guidelines may result in possible termination of HEART OF TEXAS HMIS privileges. By signing below I also acknowledge that I have received and read Hot HMIS PSOP Manual.

_____ _____ _____

System User Name | Email address | System User ID

_____

System User Signature | Date

_____

Heart of Texas HMIS Administrator Signature | Date

# HOMELESS MANAGEMENT INFORMATION SYSTEM POLICIES AND STANDARD OPERATING PROCEDURES ATTACHMENT C

# *HEART OF TEXAS HMIS*

## RELEASE OF INFORMATION FORM

## *ROI*

**Purpose:**

The Heart of Texas HMIS is a network of organizations committed to improving service delivery to people in need. By giving your consent to release your client information and information on members of your household to the HEART OF TEXAS HMIS network, you are agreeing to participate in the HEART OF TEXAS HMIS Continuum of Care program and allow the HEART OF TEXAS HMIS organizations to share and manage this information in an effort to coordinate and improve delivery of needed services, and to avoid duplication in providing basic intake information.

**Consent:**

**This release includes all partners of the HEART OF TEXAS HMIS network.**

I, _____, give my permission to allow HEART OF TEXAS HMIS organizations and their staff to release and receive client information about me *or* the client, and members of the household in order to determine eligibility for various programs and to coordinate the delivery of services. I also give permission for HEART OF TEXAS HMIS to obtain information which may determine my *or the* client's and the household's eligibility for available services and programs. I understand that the information I provide during intake, interviews, and all other correspondence with any HEART OF TEXAS HMIS organization may be shared with other HEART OF TEXAS HMIS partners for the purpose of service delivery.

I also understand that the information I provide, as well as information about the services I and my household receive, will be kept confidential by all HEART OF TEXAS HMIS organizations as required by law. I further understand that any information I provide may be used for statistical purposes by the HEART OF TEXAS HMIS network and/or any or all of its partner organizations, and that HEART OF TEXAS HMIS and its partner organizations will maintain the confidentiality of any and all personally identifiable information as required by law.

I understand that this consent is effective for ***three years*** from the date in which it is signed. Furthermore, I understand that this consent can be revoked at any time by completing a release withdrawal form at any HEART OF TEXAS HMIS agency requesting revocation of my consent. This ROI is agency specific. Therefore one will need to be completed for each HoT HMIS participating agency from which I receive services.

I understand that this release is optional, and that I and my household can still apply for and receive services, provided I am *or* the client is, and the household members are eligible, without signing this form. I understand that if I choose not to sign this form, the information will be entered into the HEART OF TEXAS HMIS system in a manner that will allow no other agency to access these client records. I understand that this information will, however, be used for statistical reporting purposes, in a non-identifying manner.

I have read, understand, and voluntarily consent to the release of my *or* the client's, and members of the household information to HEART OF TEXAS HMIS partners:

_____ _____

Client (or legal guardian) Signature Date

_____ _____

Client Social Security Number Relationship to client (if applicable)

_____ _____

HEART OF TEXAS HMIS Agency Employee Signature Date

☐ Check here if verbal consent received. HEART OF TEXAS HMIS Agency Employee must sign and date above.

# HOMELESS MANAGEMENT INFORMATION SYSTEM POLICIES AND STANDARD OPERATING PROCEDURES ATTACHMENT D

**HOMELESS MANAGEMENT INFORMATION SYSTEM**


**THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.**

**PLEASE READ IT CAREFULLY.**

## Our Duty to Safeguard Your Protected Information

_____ collects information about those who access our services. When we meet with you we will ask you for information about you and your family and enter it into a computer program called the Heart of Texas Homeless Management Information System (HoT HMIS). Although HMIS helps us to keep track of your information, individually identifiable information about you is considered "protected information". We are required to protect the privacy of your identifying information and to give you notice about how, when and why we may use or disclose any information you may give us.

We are also required to follow the privacy practices described in this Notice, although _____ reserves the right to change our privacy practices and the terms of this Notice at any time. You may request a copy of the new notice from any Heart of Texas HMIS Agency.

## How We May Use and Disclose Your Information

We use and disclose collective information for a variety of reports. We have a limited right to include some of your information for reports on homelessness and services needed by those who are homeless. Information that could be used to tell who you are will never be used for these reports. We will NOT turn your information over to a national database. For uses beyond reports, we must have your written consent unless the law permits or requires us to make the use or disclosure without your consent. **Please review the Client Release of Information Form for details. You must sign this form before we can use your information, but you do not have to sign the form in order to receive services.**

# HOMELESS MANAGEMENT INFORMATION SYSTEM POLICIES AND STANDARD OPERATING PROCEDURES ATTACHMENT E

# Universal Data Elements

HMIS Universal Data Elements are elements required to be collected by all projects participating in HMIS, regardless of funding source. The Universal Data Elements establish the baseline data collection requirements for all contributing CoC projects. They are the basis for producing unduplicated estimates of the number of people experiencing homelessness, accessing services from homeless assistance projects, basic demographic characteristics of people experiencing homeless, and patterns of service use, including information on shelter stays and homelessness over time. The Universal Data Elements are the foundation on which the Annual Homeless Assessment Report (AHAR) is developed. The AHAR provides Congress the national estimates of the current state of homelessness across the United States and the use of homeless assistance programs. It is used locally to inform state and local communities on how their specific homeless information compares nationally. The AHAR is used by the U.S. Interagency Council on Homelessness to measure progress towards goals specified in Opening Doors and by all of the federal partners to inform homelessness policy. Universal Data Elements also help local communities to better target resources, and position programs to end homelessness.

**The Universal Data Elements are:**

| | | | |
|---|---|---|---|
| 3.1 | Name | 3.917 | Living Situation |
| 3.2 | Social Security Number (SS Data Quality question also) | 3.10 | Project entry Date |
| 3.3 | Date of Birth | 3.11 | Project Exit Date |
| 3.4 | Race (Primary) | 3.12 | Destination |
| 3.5 | Ethnicity | 3.13 | Personal ID |
| 3.6 | Gender | 3.14 | Household ID |
| 3.7 | Veteran Status | 3.15 | Relationship to Head of Household |
| 3.8 | Disabling Condition (Do you have a disability of long duration? | 3.16 | Client Location |

# Program Specific Data Elements

Program Specific Data Elements differ from the Universal Data Elements in that no one project must collect every single element in this section. Which data elements are required is dictated by the reporting requirements set forth by each Federal partner for each of its programs. A Partner may require all of the fields or response categories in a data element or may specify which of the fields or response categories are required for their report. This section is organized to illustrate which Program Specific Data Elements are required by more than one Federal Partner and which are required by only one of the Federal Partners. Local CoCs may elect to require all contributing continuum projects to collect a subset of the data elements contained in this section to obtain consistent information across a range of projects that can be used to plan service delivery, monitor the provision of services, and identify client outcomes. However, these data elements do not constitute a client assessment tool, and projects must develop their own data collection protocols in order to properly assess client service needs.

**The following Program Specific Data Elements are required by more than one Federal Partner:**

4.1 Housing Status

4.2 Income and Sources

4.3 Non-Cash Benefits

4.4 Health Insurance

4.5 Physical Disability

4.6 Developmental Disability

4.7 Chronic Health Condition

4.8 HIV/AIDS

4.9 Mental Health Problem

4.10 Substance Abuse

4.11 Domestic Violence

4.12 Contact

4.13 Date of Engagement

4.14 Services Provided

4.15 Financial Assistance Provided

4.16 Referrals Provided

4.17 Residential Move-In Date

4.18 Housing Assessment Disposition

4.19 Housing Assessment at Exit

*(UDE are highlighted in **RED** throughout the system and must be answered for ALL clients)*