VENTURA COUNTY

HOMELESS MANAGEMENT INFORMATION SYSTEM (VC HMIS)

POLICIES AND PROCEDURES

February 2014

Table of Contents

1. PROJECT SUMMARY

A. Background: The Congressional Directive

A Homeless Management Information System (HMIS) refers to a system for tracking the use of homeless programs and producing an unduplicated count of the people using those programs. For FY2001, Congress directed the U.S. Department of Housing and Urban Development (HUD) to ensure that homeless programs using federal funds participate in local systems to track the use of services and housing.[1]

The Ventura County HMIS programs include:

Homeless Assistance Programs under HEARTH

- Continuum of Care
  1. Permanent Housing - (Permanent Supportive Housing and Rapid Re-Housing)
  2. Transitional Housing
  3. Supportive Services Only

- Emergency Solutions Grant (ESG)
  1. Emergency Shelter
  2. Homeless Prevention
  3. Rapid Re-Housing

Non-HUD Funded Homeless Service Programs

Programs that receive other sources of funding are not required to participate in HMIS, but are strongly encouraged to do so to contribute to a better understanding of homelessness in our communities.

To follow Congress' directive, HUD has told communities to assess their own needs and select the HMIS software that best meets those needs. HUD has provided substantial technical assistance to the Ventura County HMIS to support the planning process.

The VC HMIS is not connected to any federal or national data collection facility and data is not passed electronically to any other national database for homeless or low-income individuals.

B. Operating Procedures

Operating Procedures will provide specific policies and steps necessary to control the operational environment and enforce compliance in the areas of:

1. Provider Participation
2. User Authorization
3. Collection of Client Data
4. Release of Client Data
5. Workstation Security
6. Training
7. Technical Support

[1] See HUD Strategy for Homeless Data Collection Conference Report (H.R. Report 106-988), which indicated that "local jurisdictions should be collecting an array of data on homelessness in order to prevent duplicate counting of homeless persons and to analyze their patterns of use of assistance, including how they enter and exit the homeless assistance system and the effectiveness of the systems. HUD is directed to take the lead in working with communities toward this end and to analyze jurisdictional data within three years."

C. Organization: The Ventura County HMIS (VC HMIS)

Ventura County Human Services Agency (HSA) is the Lead Organization for the Ventura County HMIS. Ventura County HMIS has the "responsibility to establish, support and manage HMIS in a manner that will meet HUD's standards for minimum data quality, privacy, security, and other requirements for organizations participating in HMIS."

Ventura County HMIS's goal is to go beyond the HUD mandate of producing unduplicated counts of homeless persons. Our charter is to provide a comprehensive case management system that allows the Participating Agency User to draw on the collected information to make informed program decisions.

D. Mission Statement & Vision

Mission: The Ventura County HMIS goal is to go beyond the HUD mandate of producing unduplicated counts of homeless persons. Our mission is to provide a comprehensive case management system to advance the provision of quality services for homeless persons, improve data collection, and promote more responsive policies to end homelessness in Ventura County.

HMIS is designed to be an integrated network of homeless and other service providers that use a central database to collect, track and report uniform information on client needs and services. This system will not only meet Federal requirements but also enhance service planning and delivery.

Vision: To develop, implement and administer a countywide information management system that collects client level data on homeless persons and *those at risk of homelessness (per the HEARTH Act Definition)*. This HMIS system will generate reports, inform community service planning processes, increase service delivery efficiencies and, with the client's consent, provide a mechanism to share client needs for service among partnered agencies.

E. Software

Ventura County HMIS has chosen Bowman's ServicePoint product for our HMIS. The modules that are supported as of September 2013 are:

- ServicePoint, which includes:
  - ClientPoint
  - ResourcePoint
  - ShelterPoint
  - ActivityPoint
  - SkanPoint
- CallPoint
- EligibilityPoint

The software functionality tracks/records:

- Outcome Management:
  - Households
  - Entry/Exit
  - Assessments
  - Services
  - Goals
  - Referrals
- Client Demographic Data Collection (HUD)

- Client Case Management
- Information and Referral Capabilities
- Bed Maintenance, Tracking and Assignment Module
- Customized Reporting Capability
- Real Time Data Entry
- Activities Management
- Case Notes Management
- Advanced Security Features

2. PARTICIPATION REQUIREMENTS

A. Adherence to Policies

All users and agency representatives must agree to the policies in this document in order to participate in the VC HMIS. A signed agreement to do so is required of all users and Participating Agencies. This section details technical, staffing assignments and training that must be fulfilled prior to being granted access to the system.

The Policies and Procedures manual and all attachments may be amended as needed at any time. Participating Agencies will be notified of any Policies and Procedures manual changes.

B. Participation Agreements

Participating Agencies are those agencies that connect to the VC HMIS for the purposes of data entry, data editing and data reporting. Relationships between the VC HMIS and Participating Agencies are governed by any standing agency-specific agreements and/or contracts already in place. Ventura County HMIS manages the Partner Agency User Agreement and the contents of the Policies and Procedures Manual. All Participating Agencies are required to abide by the policies and procedures outlined in this manual.

Prior to obtaining access to the VC HMIS, every agency must adopt the following documents:

- Ventura County Homeless Management Information System Partner Agency User Agreement (PAUA) – The agreement made between the Participating Agency User and the VC HMIS which outlines agency responsibilities regarding their participation in the HMIS. This document is legally binding and encompasses all state and federal laws relating to privacy protections and data sharing of client specific information.
- Ventura County HMIS Client Informed Consent & Release of Information Authorization (ROI) must be implemented and monitored by agencies and would require clients to authorize in writing the entering and/or sharing of their personal information electronically with other Participating Agencies throughout the Ventura County HMIS where applicable.
- Ventura County HMIS Client Rights and Explanation of Data Uses – Client Information document to inform clients how their personal information gathered and entered into HMIS will be utilized for their benefit, should they agree to provide it.
- Ventura County Privacy Notice (PN) – Document provided to inform client the purpose of HMIS and the requirement to gather personal information.
- Ventura County HMIS Revocation of Consent
- Memorandum of Understanding (MOU) – The MOU confirms the responsibilities of the VC HMIS and the Partner Agency for ongoing HMIS activities as defined in the VC HMIS Policy and Procedures.

C. Technical Standards

The VC HMIS is responsible for each Participating Agency's oversight and adherence to the Technical Standards. All agencies will be subject to periodic on-site security assessments to validate compliance of the agency's information security protocols and technical standards. The site visit will also review how the agency uses HMIS, including
Processes and workflow related to data entry, for service improvement opportunities.
(See Appendix IV for review item checklist).
Site Assessments will ensure you are in compliance with the following Technology Standards.

Network

- High Speed internet access
  - DSL, Cable, T1 Line, etc.
  - No dial up connections
- Firewall
  - Internet security suite recommended
    - Anti-virus
    - Intrusion detection
    - Quarantine
  - Personal firewall at minimum
- Mobile devices
  - WiFi recommended
  - 4G/LTE or faster
  - No 3G or older

Device/Hardware

- Windows XP or higher
- Multicore processors
- 4 GB RAM recommended, 2 GB RAM minimum
- Video: 1024x768 minimum
- No Netscape, Mozilla, AOL etc…
- No Mac's, UNIX, Linux etc…

D. Training

All HMIS Users must complete training appropriate to their functions as described in Section 5 prior to gaining access to the VC HMIS. A minimum of one training event per contract year is required for each licensed user. Additional training may be required if there are major system upgrades and/or regulatory changes. This additional training will
be communicated as being mandatory at the time that the training is established.

VC HMIS System Administrator will be trained to provide basic user follow-up training to
Support agency staff using the VC HMIS. VC HMIS System Administrator trainers will provide periodic refresher training for other users as needed.

Training Tracks include:

- HMIS User training (new and existing users)
- Reports training
- Ethics and Confidentiality training

- Privacy and Security training
- Training related to system releases as necessary

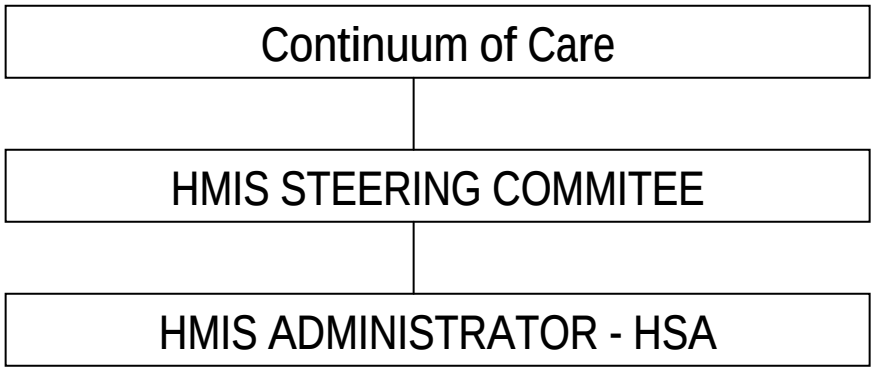
E. Participation Fees

Currently participation fees are not in place however, the Continuum of Care reserves the right to charge a participation fee to use the system.

3. SYSTEM ROLES AND RESPONSIBILITIES

A. Ventura County HMIS Organization Chart

Definitions of System Roles and Responsibilities are located under Section 10: Terminology.



4. CLIENT RIGHTS

Clients served by agencies participating in the VC HMIS have the following rights:

A. Communication

1. Clients have a right to privacy and confidentiality.
2. Clients have a right to not answer any questions unless entry into the Agency's program requires it.
3. Client information may not be shared without informed consent (posting of Privacy Notice (PN) and Mandatory Collection Notice.
4. Every client has a right to an understandable explanation of the VC HMIS and what "consent to participate" means. The explanation shall include:
   a) Type of information collected
   b) How the information will be used
   c) Under what circumstances the information will be used
   d) That refusal to provide consent to collect information shall not be grounds for refusing entry to the program.
   e) A copy of the consent shall be given to the client upon request, and a signed copy kept on file at the Participating Agency, if applicable.
   f) A copy of the Privacy Notice (PN) shall be made available upon client request.
   g) A copy of the Statement of Client Rights shall be made available upon client request.

B. Participation Opt Out

Clients have a right not to have their personal identifying information in the VC HMIS shared outside the agency, and services cannot be refused if the client chooses to opt out of participation in the HMIS. However, clients may be refused program entry for not meeting other agency eligibility criteria.

In the event that a client previously gave consent to share information in the VC HMIS and chooses at a later date to revoke consent (either to enter or to share), a HMIS Client Revocation of Consent to Release Information Form must be completed and kept on file.

C. Access to Records

A client has the right to request access to their personal information stored in the VC HMIS from the authorized agency personnel. The agency, as the custodian of the client data, has the responsibility to provide the client with the requested information except where exempted by state and federal law.

When requested, a client has the right to:

1. View his or her own data contained within the VC HMIS; No client shall have access to another client's records within the VC HMIS. An agency may not share any information about the client entered by other agencies beyond the agreed upon shared data elements.

D. Grievances

The client has the right to file a grievance with an agency. All Participating Agencies must have written grievance procedures that can be provided to a client on demand. If, after following the grievance procedure, the grievance is not resolved, the complaint may be escalated to the CoC Governing Body.

5. POLICIES FOR USERS & AGENCIES

A. User Access

User access will be granted only to those individuals whose job functions require legitimate access to the VC HMIS. Each HMIS User will attend the appropriate training course, sign a Participating Agency User Agreement and satisfy all the conditions herein before being granted access to the VC HMIS.

Explanation: The Participating Agency will determine which of their employees need access to the VC HMIS. Identified users must:

- Attend the appropriate training course for their position. For example, if the user will be case managing or entering client data, then the "New User" course would be appropriate, whereas if the person were only assigned to running reports, then the "Report Viewer" class would be appropriate.
- Sign the Participating Agency User Agreement stating that he/she has received training, will abide by the VC HMIS Policies and Procedures will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in the VC HMIS relevant to the delivery of services to people in housing crisis in the area served by the VC HMIS Collaborative.
- The signed Participating Agency User Agreement must be provided to the HMIS System Administrator prior to receipt of the user account.

B. User Activation

The HMIS System Administrator will provide unique user names and passwords to each Participating Agency user.

Explanation: User names will be unique for each user and will not be shared with other users. The HMIS System Administrator will set up a unique user name and password for each user upon completion of training and receipt of the signed Participating Agency User Agreement and the receipt of the signed acknowledgement of the Policies and Procedures Manual from each user via the Agency management. The sharing of user names will be considered a breach of the Participating Agency User Agreement and will result in *termination of the user account*.

C. Passwords

Passwords must be no less than eight and no more than sixteen characters in length, and must be alphanumeric upper and lower case with special characters. The HMIS System Administrator will communicate passwords directly to the user.

Forced Password Change (FPC): The FPC will occur every one hundred and eighty (180) consecutive days. Passwords will expire and user will be prompted to enter a new password. Users may not use the same password consecutively, but may use the same password more than once.
Unsuccessful logon: If a User unsuccessfully attempts to logon three times, the User ID will be "locked out", access permission revoked and user will be unable to gain access until their password is reset by the HMIS System Administrator in the manner stated above.

D. User Levels

1. Case Manager: This group consists of case managers who provide the day-to-day updating of client files. Case Managers will have access to all records located in Central Intake and in the Client folder, including Program Entry, Case Notes, Track Savings, Assessments, Group Services, and Program Exit.

2. Reports Only: This group includes any user at the agency who does not need to have access to client information except in report form. These reports can be canned (already built) reports, ad-hoc reports, and customized reports.

3. Agency Administrator: This group has all the access listed above, and additional access to the Agency Folder, in which they will maintain agency set-up information like program set-up, milestones, targets, and contracts/grants.

4. HMIS System Administrator: This group of top-level VC HMIS Administrators supports all agencies within the continuum and will have access to every part of the VC HMIS in order to support users.

E. Confidentiality and Informed Consent

All Participating Agencies agree to abide by and uphold all privacy protection standards established by the Ventura County HMIS as well as their respective agency's privacy procedures. The Agency will also uphold relevant Federal and California State confidentiality regulations and laws that protect client records, and the Agency will only release program level client data with written consent by the client, or the client's guardian, unless otherwise provided for in the regulations or laws.

Explanation: Participating Agencies are required to develop procedures for providing oral explanations to clients about the usage of a computerized HMIS and are required to post a Mandatory Collection Notice and a Privacy Notice (PN) in order to share Central Intake client information with other HMIS Participating Agencies. HUD Data Standards provide guidance for Participating Agencies regarding certain HMIS policies.

However, in instances of conflict between state or federal law and the HUD Data Standards, the state and/or federal law take precedence.

Oral Explanation: All clients will be provided an oral explanation stating their information will be entered into a computerized record keeping system. The Participating Agency will provide an oral explanation of the Ventura County HMIS and the terms of consent. The agency is responsible for ensuring that this procedure takes place prior to every client interview. The explanation must contain the following information, which is also included in the Client Rights and Explanation of Data Uses.

- What VC HMIS is: a web-based information system that homeless service agencies within the Ventura County Region use to capture information about the persons they serve.
- Why Gather and Maintain Data: Data collection supports improved planning and policies including determining whether desired outcomes were achieved and where more or other resources may be needed, identifying best and promising practices, and identifying factors that support or hinder achievement of outcomes.
- Security: only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records.
- Privacy Protection: No program level information will be released to another agency or individual without written consent; client has the right to not answer any question, unless entry into a program requires it; client information is stored encrypted on a central database and information that is transferred over the web is transferred through a secure connection; client has the right to know who has added to, deleted, or edited their VC HMIS record.
- Benefits for Clients: Facilitates streamlined referrals, coordinated services, unduplicated intakes and access to essential services and housing for clients.

Written Explanation: *(DRAFT Language; utilizing interim interagency data sharing agreement effective 2/12/2014)*
Each client whose program level information is being shared with another Participating Agency must agree via the Interagency Data Sharing Agreement. A client must be informed as to what information is being shared and with whom it is being shared.

- Information Release: The Participating Agency agrees not to release client identifiable information to any other organization pursuant to federal and state law without proper client consent. See attached Client Consent Form and Regulations below.
- Regulations: The Participating Agency will uphold all relevant Federal and California State Confidentiality regulations to protect client records and privacy. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in regulations, specifically, but not limited to, the following:
    - The Participating Agency will abide specifically by the federal confidentiality rules as contained in the Code of Federal Regulations (CFR) 42 Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records, regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal regulation prohibits the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by CFR 42 Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Participating Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
    - The Participating Agency will abide specifically with the Health Insurance Portability and Accountability Act of 1996 and corresponding regulations passed by the U.S. Department of Health

and Human Services. In general, the regulations provide consumers with new rights to control the release of medical information, including advance consent for most disclosures of health information, the right to see a copy of health records, the right to request a correction to health records, and the right to obtain documentation of disclosures of information may be used or disclosed. The current regulation provides protection for paper, oral, and electronic information.

- The Participating Agency will abide specifically with the California Government Code 11015.5 regarding program level Personal Information Collected on the Internet. In general, the Government Code ensures that any electronically collected personal information about clients cannot be shared with any third party without the client's written consent.

- The Participating Agency will not solicit or input information from clients unless it is essential to provide services, or conduct evaluation or research. All client identifiable data is inaccessible to unauthorized users.
- Participating Agencies are bound by all restrictions placed upon the data by the client of any Participating Agency. The Participating Agency shall diligently record in the VC HMIS all restrictions requested. The Participating Agency shall not knowingly enter false or misleading data under any circumstances.
- The Participating Agency shall maintain appropriate documentations of client consent to participate in the VC HMIS.
- If a client withdraws consent for release of information, the Agency remains responsible to ensure that the Client's information is unavailable from date of withdrawal to all other Participating Agencies.
- The Participating Agency shall keep signed copies of the Client Consent Form/Information Release form (if applicable) and/or the Interagency Data Sharing Agreement for the VC HMIS for a minimum of seven years from the date of client exit.
- Postings: Privacy Notice (PN) and Mandatory Collection Notice must be posted at the agency:
  1. The Agency must post Privacy and Mandatory Collection notices at each intake desk or comparable location.
  2. The Privacy Notice (PN) and Mandatory Collection Notice must be made available in writing at the client's request.
  3. If the agency maintains an agency website, a link to the Privacy Notice (PN) must be on the homepage of the agency's website.

F. Data Quality

HMIS Users are responsible for the ensuring VC HMIS Data Quality. Data quality refers to the timeliness, accuracy and completeness of information collected and reported in HMIS. All Participating Agencies agree to enter, at a minimum, the VC HMIS required data elements.

Explanation: Participating Agencies will collect as much relevant client data as possible for the purposes of providing services to that client. The Participating Agency agrees to input the collected data no later than one month following the month of program entry. The Participating Agency agrees to the data collection commitment by signing the Agency Agreement and is responsible for updating client's records as needed. The HMIS System Administrators will run quarterly data quality reports. Any patterns of error (including blank entries) will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to correct data entry errors and processes. Verification by the HMIS System Administrators will occur to ensure the successful correction of data entry errors and processes. Users may be required to attend additional training as needed.

- The Participating Agency shall only enter individuals in the VC HMIS that exist as Clients under the Agency's jurisdiction. The Participating Agency shall not misrepresent its Client base in the VC HMIS by entering known inaccurate information.
- The Participating Agency will not alter information in the VC HMIS that is entered by another Agency with known inaccurate information.
- The Participating Agency shall not include profanity or offensive language in the VC HMIS.
- The Participating Agency shall utilize the VC HMIS for business purposes only.
- The transmission of material in violation of any federal or California State regulations is prohibited. This includes, but is not limited to, copyright material, material legally judged to be threatening or obscene, and material considered protected by trade secrets.
- The Participating Agency shall not use the VC HMIS with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.

The HMIS Program Manager may request that the local CoC Governing Body sanction any user and/or Participating Agency found to be in violation of the requirements of this section. If necessary, sanctions by the loval CoC include, but not limited to:

- A formal letter of warning to the Agency
- Suspension of system privileges
- Revocation of system privileges

The Participating Agency or End User has the right to file a Grievance regarding Sanctions from the HMIS Program Manager/CoC Governing Body. The HMIS Steering Committee will review the grievance, research the nature of the infraction, and will respond to the grievant within 30 days.

G. Data Use by Ventura County HMIS

The Continuum within the Ventura County HMIS shall have access to its respective agencies' client data contained within the VC HMIS.

Explanation: For the purposes of system administration, user support, and program compliance, VC HMIS will use the data contained within the VC HMIS for analytical purposes only and will not disseminate client-level data. The Continuum may release aggregate data contained within the VC HMIS for research and regional reporting purposes only. The System Administrator Agreement must be signed by all HMIS System Administrators.

H. Data Use by Vendor

The Vendor and its authorized subcontractor(s) shall not use or disseminate data contained within the VC HMIS.

Explanation: To enforce information security protocols and to ensure that VC HMIS data is used only with explicit permission and if permission is granted, will only be used in the context of interpreting data for research and for system troubleshooting purposes, the contract signed by the HMIS Lead Agency and the software vendor contains language that prohibits access to VC HMIS data.

I. Data Use by Agency

Data contained in the VC HMIS will only be used to support the delivery of services to at risk and homeless clients in the VC areas. Each HMIS User will affirm the principles of ethical data use and client confidentiality as noted below and contained in the HMIS User Agreement.

Explanation: As the guardians entrusted with client personal data, HMIS Users have a moral and a legal obligation to ensure that the data they collect is being gathered, accessed and used appropriately. It is also the responsibility of each user to ensure that client data is only used to the ends to which it was collected, ends that have been made explicit to clients and are consistent with the mission of the agency and the VC HMIS to assist families and individuals to resolve their housing crisis. Proper user training, adherence to the VC HMIS Policies and Procedures Manual, and a clear understanding of client confidentiality are vital to achieving these goals. All HMIS Users will sign an HMIS User Agreement before being given access to the system. Any individual or Participating Agency misusing, or attempting to misuse the VC HMIS data can be denied access to VC HMIS. Sanctions exist if users violate any laws related to client confidentiality, as outlined in Section 8: Violations.

J. Maintenance of Onsite Computer Equipment

Participating Agencies commit to a reasonable program of data storage and equipment maintenance in order to sustain an efficient level of system operation. Participating Agencies must meet the technical standards for minimum computer equipment configuration; Internet connectivity, antivirus and firewall.

Explanation: The Participating Agency Leadership designee will be responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the VC HMIS including the following:

1. Computer Equipment: The Participating Agency is responsible for maintenance of onsite computer equipment. This includes the following:
    - Purchase of and upgrades to all existing and new computer equipment for utilization in the VC HMIS.
    - Workstation(s) accessing the VC HMIS must have a locking, password-protected screen saver
    - All workstations and computer hardware (including agency network equipment) must be stored in a secure location (locked office area)
2. Data Storage: The Participating Agency agrees to only download and store data in a secure environment. Refer to Section 2.C: Technical Standards for more information.
3. Data Disposal: The Participating Agency agrees to dispose of documents that contain identifiable client level data by shredding paper records, deleting any information from diskette before disposal, and deleting any copies of client level data from the hard drive of any machine before transfer or disposal of property.

K. Downloading of Data

HMIS Users will maintain the security of any client data extracted from the VC HMIS and stored locally, including all data contained in custom reports. HMIS Users may not electronically transmit unencrypted client data across a public network.

Explanation: To ensure that the VC HMIS is a confidential and secure environment, data extracted from the VC HMIS and stored locally will be stored in a secure location and will not be transmitted outside of the private local area network unless it is properly protected. Security questions can be addressed to the HMIS System Administrator. Any personally identifiable information will not be distributed through email.

L. Data Sharing

(DRAFT Language; utilizing interim interagency data sharing agreement effective 2/12/2014)

Basic client information within the system will be shared based upon the level of consent designated by the client within the VC HMIS. A Client may choose to limit the period of time for which their data will be shared.

Explanation: Data sharing refers to the sharing of information between Participating Agencies for the coordination of case management and client service delivery. Specific data elements to be shared are limited to those as outlined in HMIS Data and Technical Standards Final Notice – (69 FR 146), as revised in HMIS Data Standards Revised Notice-March 2010, Section 1.6. This includes: Universal Data Elements, Household Demographics, Employment and Education Information.

Program level information in either electronic or paper form will never be shared outside of originating agency without written client consent. Information that is shared with written consent will only be used for the purpose of service delivery. End users found to be sharing program level client data without written consent will have their access terminated.

M. Data Release

Aggregate level (client de-identified) data may be released by Agencies, the local Continuum of Care and/or by the Ventura County HMIS under certain criteria. Client-level data may only be released by written consent from the client for a specified purpose.

Explanation: Data release refers to the dissemination of aggregate and/or client-level information for statistical, analytical, reporting, advocacy, regional needs assessment, trend analysis, etc.

1. Agency Release: Each Participating Agency owns all data it enters into the VC HMIS. The agency may not release any client level information without the express written consent of the client. Agencies may release program and/or aggregate level data for all clients to whom the agency provided services with the express written permission of the CoC or assigned authorized entity. No individual client data will be provided to any group or individual that is neither the Participating Agency that entered the data nor the client without proper authorization or consent by the client. This consent includes the express written authorization for each individual or group requiring access to the client's data.

2. Continuum of Care Release: The Continuum of Care (CoC) may release aggregate information about the Continuum at the program, sub-regional and regional level. Continuum level aggregate data may be released without agency permission at the discretion of the agency's continuum. The VC HMIS will not release agency- or client- specific data to outside groups or individuals.

3. Ventura County HMIS Release: The Ventura County HMIS, with the consent of the CoC, will develop an annual release of aggregate data in a summary report format, which will be the standard response for all requests for collaborative data. The Ventura County HMIS will not release agency- or client- specific data to outside groups or individuals.

N. Agency Customization

A Participating Agency will have the ability to request system customization at the Agency level to reflect the data collection needs for their specific programs(s). The VC HMIS contains certain fields that can be tailored at no cost to the agency. Additional customization as performed by the software vendor or VC HMIS System Administrators may be purchased at the expense of the agency.

Explanation: Participating Agencies have some ability to customize VC HMIS fields to meet the specific needs of their program at the discretion of the Continuum of Care (CoC). At the request of the Agency

Administrator, the HMIS System Administrator will evaluate the request and implement the changes as warranted.

6. TECHNICAL SUPPORT AND SYSTEM AVAILABILITY

A. Technical Support

The Ventura County HMIS will provide technical support to all Agency Administrators and HMIS Users as needed.

Explanation: The Agencies that have an Agency Administrator are expected to provide first level technical support. The Ventura County HMIS System Administrators will provide all other technical support to the Agency Administrators and HMIS Users.

Technical Support Hours – 8:00 a.m. – 5:00 p.m. (PST), Monday through Friday (Excluding Holidays).
While the winter warming shelter is active, after hours support is negotiated.
Staff will respond in a timely manner to any requests for support made during the above hours. For technical support, please contact:
Ventura County HMIS telephone number: (805) 477-5156
HMIS-Support@ventura.org

Assistance will be provided in the following areas:

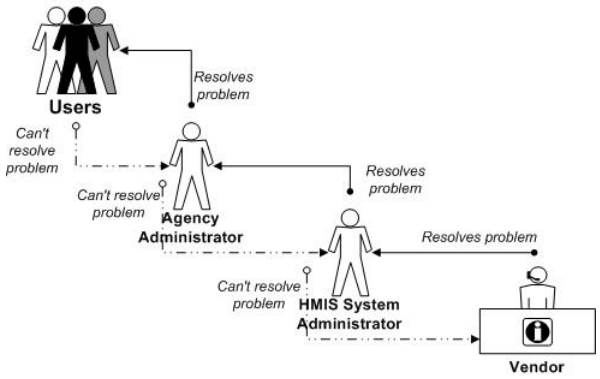
- Help Desk Support: Help Desk support is provided to help HMIS Users access and utilize HMIS application.
- Training: Agency Administrator training, User training, and Report training is provided quarterly. The schedule is posted one month in advance of the training and registration instructions are provided once the schedule is posted.
- System Customization: HMIS contains certain fields that can be tailored at no cost to the agency.
- Reporting: Training and technical assistance in accessing standardized reports and the creation of ad hoc (custom reports).
- Data Analysis: Interpreting reports.

Additional costs may apply in the following areas:

- System Customization: Agency-specific customization requests.
- Reporting: Agency-specific customized reports.
- Data Conversion: Assist in the development of a data conversion/migration plan, and provide support in data conversion/migration implementation.
- Data Analysis: Extensive analysis of agency's data.

Requests should be delineated as follows:

Technical Assistance Flow Chart



B. System Availability and Scheduled Maintenance

The Ventura County HMIS will be available to users at a minimum of 97.5% of the year.

Explanation: Necessary downtime for HMIS upgrades and patches will be communicated by HMIS System Administrators system-wide and performed in the late hours when possible.

C. Unplanned Interruption to Service

In the event of unplanned interruption to service, HMIS System Administrators will notify all Participating Agencies as soon as possible.

Explanation: When an event occurs that makes HMIS inaccessible, the HMIS System Administrator will analyze and determine the problem. In the event it is determined that HMIS accessibility is disabled system-wide, then the HMIS System Administrators will work with the software vendor to repair the problem. Within two hours of problem awareness, Participating Agencies will be informed of the estimated system availability. HMIS System Administrators will notify Participating Agencies via e-mail when service has resumed.

D. Conversion of Existing Data

Data migration from legacy systems is allowed upon approval from the local HMIS System Administrators. Migrated data must be non-duplicated and an exact match to the existing HMIS field type. The Participating Agency is responsible for the accuracy, completeness and quality of the migrated data.

Explanation: Data migration (or conversion) is the one-time process of transferring data from any existing system to the Ventura County HMIS. Upon transfer, the agency abandons its existing system and uses Ventura County HMIS for recording all client-related data.

The Agency's existing system must be an ODBC-compliant database platform in order for migration to be possible. The HMIS System Administrator can help the Agency determine the ODBC compatibility for any legacy systems. Only data that is an exact match with VC HMIS data fields may be migrated. Data must be unduplicated prior to data migration. All required fields in the VC HMIS are required for migration. A data dictionary will be provided upon request. This activity is provided by the System Vendor and will incur an additional cost. Cost will be determined prior to the service being rendered and will be agreed upon by requesting Agency, CoC Lead and Program Manager.

If the agency's data cannot be migrated, manual conversion (data entry by the agency's personnel) may be necessary to move data from legacy systems into the Ventura County HMIS.

7. SYSTEM ARCHITECTURE & SECURITY

A. Password Management Procedure

An HMIS End User must notify the Agency Administrator or HMIS System Administrator immediately upon realization that his or her password has been lost, forgotten or made public to others. The Agency Administrator is responsible for notification of password breach to the HMIS System Administrator. Upon notification, the HMIS System Administrator will immediately reset the user's password. A new HMIS End User will not receive an initial password without training.

Explanation: The HMIS System Administrator will reset the user password. The new password will be valid from the time of the reset until the next logon.

- Passwords need to be 8 characters minimum and contain a number, upper and lowercase letters, and 1 or more special characters.
- Passwords expire after 60 days (after expiration interval the user is required to provide a new password upon logon)
- Passwords cannot be reused.
- If system is dormant for 20 minutes, user will be forced to log back in.

B. Virus Protection

Agency Responsibilities: All Participating Agency computers and networks must have up-to-date anti-virus software.

Explanation: All Participating Agency computers should be protected by anti-virus software. The anti-virus software should be updated regularly to maintain maximum protection from the most recently released viruses.

C. Backup and Recovery Procedures

Ventura County HMIS is routinely backed up and saved to redundant systems by the vendor pursuant to the contract term and agreement to prevent loss of data.

D. Auditing and Monitoring

HMIS System Administrators have access to activity logs of changes made to the information contained within the database by end users. HMIS System Administrators can upon request or notice of suspicious/questionable behavior monitor access to the system by an end user that could potentially reveal a violation of information security protocols. Any request for auditing and monitoring will be evaluated for justification, investigated, and be kept confidential.

8. VIOLATIONS

A. Right to Deny Access

The HMIS System Administrator has the right to deny user access to the HMIS if an end user has violated any of the policies in this document. Any user or Participating Agency suspected of violating a policy may be subject to suspension of HMIS privileges until the violation can be resolved.

Explanation: If deemed necessary for the immediate security and safety of Ventura County HMIS data, the HMIS System Administrator has the right to deny or revoke user access to HMIS. The HMIS System Administrator will report access revocations to the HMIS Program Manager. The HMIS Program Manager will report all revocations to the CoC, HMIS Steering Committee and the Participating Agency.

B. Reporting a Violation

HMIS Users should report any suspected or alleged privacy or security violations to the HMIS System Administrator immediately.

Explanation: All HMIS Users are obligated to report suspected instances of noncompliance. For the Agencies that have an Agency Administrator, users should report security violations to the Agency Administrator first and then the Agency Administrator has the responsibility of providing that information to the HMIS System Administrator. If the Agency does not have an Agency Administrator, then the HMIS User is to report violations to the HMIS System Administrator directly.

C. Possible Sanctions

The HMIS Program Manager may request that the local CoC Governing Body sanction any user and/or Participating Agency found to be in violation of the privacy and/or security protocols.

Sanctions by the local CoC include, but are not limited to:

- A formal letter of reprimand
- Suspension of system privileges
- Revocation of system privileges
- Recommendation for corrective action for employee
- Referral for potential criminal prosecution

9. GRIEVANCES

A. Client Grievance Process

Clients will contact the Participating Agency with which they have a grievance for resolution of VC HMIS problems. Participating Agencies will report all client grievances to the local CoC Governing Body.

Explanation: Each Participating Agency is responsible for answering questions and responding to grievances from their own clients regarding the VC HMIS. After client has brought a VC HMIS-related complaint to the Participating Agency, the Participating Agency must have a process to respond to the complaint. The Participating Agency will provide a copy of the portion of the VC HMIS Policies and Procedures and the Client Revocation of Consent to Release Information to the client.

The Participating Agency must keep all grievances and responses on file at the agency site. The Participating Agency will send written notice of the grievance and response to the grievance to the local CoC Governing Body. The HMIS System Administrator will record all grievances and report them to the VC HMIS Steering Committee. Appropriate action will be taken as required by the local CoC Governing Body.

The CoC has overall responsibility for their local VC HMIS effectiveness and will respond if users and/or Participating Agencies fail to follow the terms set forth in the VC HMIS Policies and Procedures Manual, Agency Agreements, and User Agreement or if a breach of client confidentiality or the intentional misuse of client data occurs.

B. Agency Grievance Process

Participating Agencies will report all agency-generated VC HMIS-related grievances to the local CoC Governing Body. If the grievance is related to a problem with the VC HMIS, it must be reported to the HMIS System Administrator. Corrective action will be taken if system-wide changes are warranted.

Explanation: In order for the VC HMIS to serve as an adequate tool for agencies and provide a more accurate picture of our region's homelessness, any grievances related to problems with the VC HMIS must be addressed by the agency in conjunction with the CoC Governing Body with the goal of affecting systemic change where necessary. The local CoC will report grievance problems to the HMIS Administrator. If system-wide changes are warranted for a corrective action, it will be forwarded to the HMIS Steering Committee for approval.

The Participating Agency or End User has the right to file a Grievance regarding Sanctions from the HMIS Program Manager/CoC Governing Body. The HMIS Steering Committee will review the grievance, research the nature of the infraction, and will respond to the grievant within 30 days.

10. TERMINOLOGY

Agency Administrator: The person responsible for some system administration at the agency level. Responsibilities include informing HMIS System Administration of the need to add and delete users, basic trouble-shooting, and escalation of issues to their HMIS System Administrator. This person is the agency user's first line of contact for HMIS issues.

Agency Executive Management: The high-level management staff that is responsible for organization level decision making, for example, the agency President or Executive Director.

Aggregate Data: Data with identifying elements removed and concentrated at a central server. Aggregate data are used for analytical purposes and reporting.

Anti-Virus Software: Programs to detect and remove computer viruses. The anti-virus software should always include a regular update services allowing it to keep up with the latest viruses as they are released.

Application Service Provider (ASP): A 3rd party entity that manages and distributes software-based services to customers across a wide area network.

Audit Trail: A history of all access to the system, including viewing, additions and updates made to a client record.

Authentication: The process of identifying a user in order to grant access to a system or resource. Usually based on a username and password.
Cable: A type of modem that allows people to access the Internet via their cable television service.

Coordinated Assessment Level Data: Client information collected at intake, including the following system screens: Client Intake, Household/Demographics, Referral, Eligibility, Education/Employment and Documents.

Customer: The person receiving services whose information is entered into HMIS.

Continuum of Care (CoC): Continuum of Care; refers to the range of services (outreach, emergency transitional and permanent housing and supportive services) available to assist people out of homelessness.

CoC Governing Body: the entity responsible for policy decisions for a Continuum of Care system.

Database: An electronic system for organizing data so it can easily be searched and retrieved. The data within the HMIS is accessible through the web-based interface.

Decryption: Conversion of scrambled text back into understandable, plain text form. Decryption uses an algorithm that reverses the process used during encryption.

Dedicated IP: a reserve IP (see IP)

Dynamic Host Configuration Protocol (DHCP): A protocol that provides a means to dynamically allocate IP addresses to computers on a local area network (LAN).
Digital Certificate: An attachment to a message or data that verifies the identity of a sender.

Digital Subscriber Line (DSL): A digital telecommunications protocol designed to allow high-speed data communication over the existing copper telephone lines.

Encryption: Conversion of plain text into encrypted data by scrambling it using a code that masks the meaning of the data to any unauthorized viewer. Encrypted data are not readable unless they are converted back into plan text via decryption.

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.

HMIS: Homeless Management Information System. This is a generic term for any System used to manage data about the use of homeless services.

HMIS System Administrator: The person(s) with the highest level of user access. This user has full access to all user and administrative functions in the CoC and will serve as the liaison between Participating Agencies and the vendor. There is at least one HMIS System Administrator in each CoC.

HMIS User: A person who has a unique user identification (ID) and directly accesses HMIS to assist in data collection, reporting or administration as part of their job function in homeless service delivery. Users are classified as either system users who perform administration functions at the system or aggregate level or agency users who perform functions at the agency level.

Host: A computer system or organization that plays a central role providing data storage and/or application services for HMIS.

Internet: A set of interconnected networks that form the basis for the World Wide Web.

Internet Protocol Address (IP Address): A unique address assigned to a user's connection based on the TCP/IP network. The Internet address is usually expressed in dot notation, e.g.: 128.121.4.5.

Internet Service Provider (ISP): A company that provides individuals or organization with access to the internet.

Local Area Network (LAN): A network that is geographically limited, allowing easy interconnection of computers within offices or buildings.

Network: Several computers connected to each other.

Network Address Translation (NAT) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

On-site: The location that uses the HMIS and provides services to at-risk and homeless clients.

Participating Agency: An agency, organization, or group that has signed an

HMIS Agency Agreement with their respective CoC Governing Body.

Program Level Data: Client information collected during the course of the client's program enrollment, including the following system screens: Program Entry, Services Provided, Client Profile, Case Notes, Track Savings, Bed Assignments, Bed Maintenance, Daily Services, Sessions, and Program Exit.

Real-Time: Data that is processed and available to other users as it is entered into the system.

Server: A computer that provides a service for other computers connected to it via a network. Servers can host and send files, data or programs to client computers.

Static IP Address: see Dedicated IP
T1 Line: Communication line that can carry voice or data at transmission speeds that are 25 times the speed of a modem.

Transmision Control Protocol/Internet Protocol (TCP/IP) –The protocol that enables two or more computers to establish a connection via the internet.

User ID: The unique identifier assigned to an authorized HMIS User.

Virtual Private Network (VPN): A group of computer systems that communicate securely over a public network.

Wide Area Network (WAN): A network that is not geographically limited, can link computers in different locales, and extend requests for web pages.

Wired Equivalent Privacy (WEP): is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) Standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (LAN) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.

11. ACKNOWLEDGEMENT

I acknowledge that I have received a written copy of the Ventura County HMIS Policies and Procedures. I understand the terms of the Ventura County HMIS Policies and Procedures and I agree to abide by them. I understand that any violation of the policies or procedures could lead to CoC sanctions or even criminal prosecution.

Agency Name:_____

Printed Name:_____

Signature:

Date: