OFFICE OF HOMELESS SERVICES

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

POLICY AND PROCEDURE HANDBOOK

Participation Eligibilities

Introduction

The Department of Housing and Urban Development (HUD) recognized that implementing a Homeless Management Information System (HMIS) is a difficult and time-consuming process, and must necessarily be done in stages. Participation eligibilities and priories were determined by the following:

- First priority is to bring on board emergency shelters, transitional housing programs, and outreach programs. Providers of emergency shelter, transitional housing, and homeless outreach services should be included in the HMIS as early as possible, regardless of whether they receive funding through the McKinney-Vento Act or from other sources.
- As a second priority, HUD encourages the Continuum of Care (CoC) to actively recruit providers of permanent supportive housing funded by HUD McKinney-Vento Act programs and other HUD programs.
- As a third priority, CoC should recruit homeless prevention programs, Supportive Services Only programs funded through HUD's Supportive Housing Program, and non-federally funded permanent housing programs.

Participation Requirements

Adherence to policies

All Homeless Management Information System (HMIS) participating agencies must agree to the policies in this document in order to participate in the San Bernardino County Continuum of Care (SBC CoC) HMIS. A signed agreement is required of all end users and participating agencies. This section details technical, staffing assignments and training that must be fulfilled prior to being granted access to the system.

This Policies and Procedures Manual and all attachments may be amended as needed at any time. Participating Agencies will be notified of any changes and/or amendments to the Policies and Procedures Manual.

Participating Agencies

Participating Agencies are homeless service providers and other Referring Agencies that utilize SBC CoC HMIS for the purposes of data entry, data editing, data reporting and referral. Relationships between the SBC CoC and Participating Agencies are governed by any standing agency-specific agreements or contracts already in place, the HMIS Participating Agency Memorandum of Understanding (MOU), and the contents of the HMIS 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 SBC CoC HMIS, every agency must adopt the following documents:

- Housing and Urban Development (HUD) Data and Technical Standards
- HMIS Participating Agency MOU – The agreement made between the Participating Agency Executive Management and the Office of Homeless Services (OHS), which outlines agency responsibilities regarding 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.
- Interagency Data Sharing Agreement – Must be established between agencies if sharing of client level data above and beyond the minimum shared elements (Central Intake) is to take place.
- Client Consent/Information Release Forms- To 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 SBC CoC HMIS where applicable.
- HMIS End-User Policies and Procedures- Signed by each HMIS End-User and the user will agree to abide by standard operating procedures and ethics of HMIS.
- Privacy Notice – Each Participating Agency will post a written explanation describing the agency's privacy policies regarding data entered into SBC CoC HMIS.
- Client Revocation of Consent to Release Information Form- Client revokes permission to share or release personal information in SBC CoC HMIS.

Continued on next page

Participating agency (continued)

- **Grievance Form** - The client has a right to file with the HMIS Lead Organization if he/she feels that the Participating Agency has violated his/her rights.
- **Transfer of Data Agreement** (if applicable) - The agreement made between the Participating Agency Executive Director and OHS to integrate, upload, or migrate data from the agency's existing system to SBC CoC HMIS.
- **Termination of Employee** - This form is to notify the HMIS System Administrator that the referenced employee will no longer work for the organization and thus all access to the HMIS needs to be revoked.

All agencies will be subject to periodic on-site security monitoring to validate compliance of the agency's information security protocols and technical standards.

Technical standards

OHS, as the HMIS Lead Organization is responsible for each Participating Agency's oversight and adherence to HUD's Technical Standards as follows:

High Speed internet access:

- DSL, Cable, T1 Line, etc.
- No dial up connections
- Dedicated IP address is recommended
  - DHCP may be used
  - Static IP address will be required if the administrative burden of using DHCP becomes too great

PC w/ Internet Explorer 5.5 or higher:

- No Netscape, Mozilla, AOL, etc.
- No Mac's, UNIX, Linux, etc.

Microsoft .NET Framework Version 2.0 or higher:

- Can be downloaded from www.microsoft.com/downloads
- Windows NT sp6a, Windows XP
- If running XP we recommend running SP2

Firewall:

- Must use Network Address Translation (NAT) behind firewall
- If wireless is used must be protected with at minimum Wired Equivalent Privacy (WEP)
- Must be placed between any internet connection and PC for the entire network

Antivirus on ALL systems connected to an agency's network:

- Must have most recent Virus Security Updates
- This includes systems which Terminal or VPN into the network

Continued on next page

Staffing responsibilities

Each Participating Agency will need to have staff to fulfill the following roles. The responsibilities assigned to these individuals will vary. However, all functions must be assigned and communicated to the HMIS System Administrator.

Role	Functions
Executive Management *Oversight responsibility for all activities associated with agency's participation in OHS*	• Signs the **HMIS Participating MOU** and any other required forms prior to accessing SBC CoC HMIS. • Authorizes data access *to* agency staff and assigns responsibility for custody of the data. • Establishes, adopts and enforces business controls and agrees to ensure organizational adherence to SBC CoC HMIS Policies and Procedures. • Communicates control and protection requirements to HMIS Users and other agency staff as required. • Assumes responsibility for the integrity and protection of client-level data entered into the system. • Assumes liability for any misuse of the software by agency staff. • Assumes responsibility for posting **Privacy Notice**. • Assumes the responsibility for the maintenance and disposal of on- site computer equipment. • Provides written permission to the HMIS System Administrator to perform the decryption of data to upgrade SBC CoC HMIS technology. • Provides written permission to the HMIS System Administrator to perform the decryption of agency data to upgrade SBC CoC HMIS database server to new technology when the database becomes obsolete. • Periodically reviews system access control decisions.
Outcome/Program Manager and/or Agency Administrator *Internal agency resource for outcome management planning and implementation*	• Serves as the liaison between agency managers, HMIS Users and Outcome Specialists. • Attends required Outcomes Management training, Agency Administrator training, and Technical Assistance (TA) sessions. • Develops and enters into SBC CoC HMIS the outcome performance targets and milestones. • Reports system problems and data-related inconsistencies to HMIS System Administrator or Outcome Specialist as needed. • Attends HMIS End User Meeting.

Continued on next page

Staffing responsibilities (continued)

Role	Functions
HMIS End User	• Completes training on the appropriate use of SBC CoC HMIS prior to accessing the system. • Acknowledges an understanding of this Policies and Procedures Manual. • Adheres to any agency policies that affect the security and integrity of client information. • Is responsible for SBC CoC HMIS Data Quality. Data quality refers to the timeliness of entry, accuracy and completeness of information collected and reported in HMIS. • Signs **HMIS End-User Policies and Procedures** and any other required forms prior to accessing system. • Reports system problems and data-related inconsistencies to Agency Administrator or Outcome Manager as appropriate. • If applicable, obtains client signature on **Client Consent/Information Release Form**. • Gives client written copy of Statement of Client Rights. • Verbally communicates client's rights and uses of client's data.

Training

All HMIS Users must complete training appropriate to their functions as described in Item B. Staff Responsibilities prior to gaining access to SBC CoC HMIS. OHS will provide training to all users at the beginning of the agency's SBC CoC HMIS implementation and periodic refresher training for other users as needed.

Identified training tracks include:

- Outcomes Management Training
- Privacy/Ethics Training
- Data Security Training
- Data Quality Training
- HMIS User's Training
- Bed Utilization Training
- Report Training

Client Rights

Introduction

Clients served by agencies participating in the San Bernardino County Continuum of Care (SBC CoC) Homeless Management Information System (HMIS) have the rights described in this section.

Communication

Communication rights include the following:

- Clients have a right to privacy and confidentiality.
- Clients have a right to not answer any questions unless entry into the Agency's program requires it.
- Client information may not be shared without informed consent (posting of **Privacy Notice** and **Mandatory Collection Notice**).
- Every client has a right to an understandable explanation of SBC CoC HMIS and what "consent to participate" means. The explanation shall include:
  - Type of information collected.
  - How the information will be used.
  - Under what circumstances the information will be used.
  - That refusal to provide consent to collect information shall not be grounds for refusing entry to the program.
  - 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.
  - A copy of the Privacy Notice shall be made available upon client request.
  - A copy of the Statement of Client Rights shall be made available upon client request.

Participation opt out

Clients have a right not to have their personal identifying information in SBC CoC 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 SBC CoC HMIS and chooses at a later date to revoke consent (either to enter or to share), a **Client Revocation of Consent to Release Information Form** must be completed and kept on file.

Access to records

A client has the right to request access to his/her personal information stored in SBC CoC 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:

- View his or her own data contained within SBC CoC HMIS, or
- Receive a printed copy of his or her own data contained within SBC CoC HMIS.

Continued on next page

Client Rights, Continued

Access to records (continued)	No client shall have access to another client's records within SBC CoC HMIS. However, parental/guardian access will be decided based upon existing agency guidelines. The information contained in the Central Intake section of SBC CoC HMIS can be provided at any agency the client requests it from, as long as the client has previously given the other agency consent to share and that consent is still in force.
Grievances	The client has the right to file a grievance with Participating 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 Office of Homeless Services (OHS) (See Appendix for Grievance Form).

User access

User access will be granted only to those individuals whose job functions require legitimate access to the San Bernardino County Continuum of Care (SBC CoC) Homeless Management Information System (HMIS). Each HMIS End-User will satisfy all the conditions herein and have signed the HMIS End-User Policies and Procedures before being granted access to SBC CoC HMIS.

Explanation:The Participating Agency will determine which of its employees need access to SBC CoC HMIS. Identified users must sign the HMIS End-User Policies and Procedures stating that they have received training, will abide by SBC CoC HMIS Policies and Procedures, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in SBC CoC HMIS relevant to the delivery of services to homeless people in the area served by SBC CoC HMIS. The Agency Administrator will be responsible for the distribution, collection and storage of signed HMIS End-User Policies and Procedures. The existence of signed HMIS End-User Policies and Procedures will be verified and a copy obtained during the onsite review process by the HMIS System Administrator.

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 HMIS End-User Policies and Procedures and the receipt of the signed acknowledgement of the Policies and Procedures Manual from each user via the Agency Administrator. The sharing of user names will be considered a breach of the HMIS End-User Policies and Procedures.

Passwords

Passwords must be no less than eight and no more than sixteen characters in length, and must be alphanumeric with upper and lower case and characters. The HMIS System Administrator will communicate passwords directly to the end-user. Agency Administrators will contact the HMIS System Administrator to reset a user's password.

Forced Password Change (FPC): The FPC will occur every one hundred and eighty (180) consecutive days. Passwords will expire and user wH: 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 his/her password is reset by the HMIS System Administrator in the manner stated above.

Continued on next page

User levels

Central Intake Data Entry: This group consists of the front line intake workers. They will have access to the Central Intake forms in order to intake a client, enter household demographics, and make a referral.

Client Referral: This group includes any user at the agency who needs to refer the client to services. They will have access to Central Intake and the Referral Pages only.

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, Referral, Track Savings, Assessments, Group Services, and Program Exit.

Agency Administrator: The Agency Administrator 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.

HMIS System Administrator: The HMIS System Administrator is the top-level of support for all SBC CoC HMIS agencies within the continuum and will have access to every part of SBC CoC HMIS in order to support users.

Confidentiality and Informed Consent

All Participating Agencies agree to abide by and uphold all privacy protection standards established by SBC CoC 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: SBC CoC HMIS 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** in order to share central intake client information with other HMIS Participating Agencies. Housing and Urban Development (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 and Technical Standards, the state and/or federal law take precedence.

Continued on next page

Confidentiality and Informed Consent (continued)

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 SBC CoC 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 **"Privacy Notice":**

- What SBC CoC HMIS is: A web-based information system that homeless service agencies within the SBC CoC use to capture information about the persons they served.
- 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 his/her SBC CoC HMIS record.
- Benefits for clients: Facilitates streamlined referrals, coordinated services, unduplicated intakes and access to essential services and housing.

Written Explanation: Each client whose program level information is 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 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 (following).

Continued on next page

Confidentiality and Informed Consent (continued)

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, 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 SBC CoC 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 SBC CoC HMIS.

Continued on next page

Confidentiality and Informed Consent (continued)

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 or for SBC CoC HMIS for a minimum of seven years from the date of client exit.

Postings: Privacy and Mandatory Collection Notices must be posted at the agency:

- The Agency must post **Privacy and Mandatory Collection Notices** at each intake desk or comparable location.
- The **Privacy** and **Mandatory Collection Notice** must be made available in writing at the client's request.
- If the agency maintains an agency website, a link to the **Privacy Notice** must be on the homepage of the agency's website.

Data integration

Explanation: HMIS data integration refers to the data that is integrated from a SBC CoC agency that is currently collecting client level data in a HMIS data system other than the current software that is being utilized by the SBC CoC HMIS Participating Agencies. Agencies who agree to integrate data will complete and sign the **San Bernardino HMIS Participating Agencies Data Integration Memorandum of Understanding** document.

Data quality

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

Explanation: HMIS data quality refers to the extent that data recorded in the SBC CoC HMIS accurately reflects the same information in the real world. Participating Agencies need to adopt HUD's data quality standards in order to help SBC CoC better understand and address homelessness in San Bernardino County. Data quality refers to the timeliness, accuracy, completeness and consistency of information collected and reported in SBC CoC HMIS.

Data Timeliness: To be most useful for reporting, an HMIS should include the most current information about the clients served by participating homeless programs. To ensure the most up to date data, information should be entered by the user as soon as it is collected. Intake data needs to be added within two working days of the intake process or client encounter. Information that tends to change periodically also needs to be regularly verified and/or updated, such as information on income sources and amounts.

Continued on next page

Data quality (continued)

Using Paper-based Data Collection Forms: Agencies may choose to collect client data on paper and enter it into the HMIS software later, rather than entering it directly in the system. If data is collected by paper first, that information must be entered into the HMIS system within two days. Each agency will incorporate HMIS into its own operating processes; some agencies will prefer to interview clients and simultaneously enter their information directly into the computer, other agencies will find it easier to collect information on paper first, and then have someone enter the data later. Agencies may utilize the HMIS paper-based forms for initial data collection. Agencies will have two (2) calendar days from the point of the event (intake/enrollment), service delivery, or discharge) to record the information into the HMIS software.

The HMIS Lead Agency strongly recommends that all agencies that enter data into the HMIS complete the program specific data fields even if the funding received by the agency does not dictate they do so. The additional data points on the client will prove extremely helpful for the agency when reporting on client outcome measurement/progress, internal accounting for service delivered, and external reporting to funders.

Continued on next page

Data quality (continued)

Data Accuracy: Information entered into the HMIS needs to be valid, i.e. it needs to accurately represent information on the people that enter any of the homeless service programs contributing data to the SBC CoC HMIS.

Data Completeness: To release meaningful information from the SBC CoC HMIS, data needs to be as complete as possible, i.e., it should contain all required information on all people served in the program (i.e., emergency shelter) during a specified time period. On the macro level, the goal of achieving adequate HMIS coverage and participation by all local programs is essentially about ensuring that the records are representative of all the clients served by these programs. If a client record is missing, then aggregate reports may not accurately reflect the clients served by the program. Similarly, if an entire program is missing, data from the SBG CoC HMIS may not accurately reflect the homeless population in the community.

Data Consistency: HMIS end-user must have an understanding of what data need to be collected and in which way. Different interpretations of how questions for data collection should be asked or a lack of understanding of what answers to questions mean lead to aggregate information that cannot be correctly interpreted and presented.

CoC Programs: HUD now requires that all CoC Programs, especially those that house homeless individuals (Homeless Assistance Programs) and are identified on the CoG's Housing Inventory Chart collect universal data and program information on all clients served by CoG Programs regardless of whether the program participates in the HMIS. The following Universal and Program Specific Data Elements must be captured and input into HMIS for each client served including children in all Emergency Shelter Programs, Emergency Solutions Grant, Supportive Housing Program Veteran's Supportive Housing, and Housing Opportunities for People with AIDS:

- Name
- Social Security Number
- Date of Birth
- Race
- Ethnicity
- Veteran Status
- Disabling Condition
- Gender
- Residence Prior to Program Entry
- Zip Code of Last Permanent Address
- Program Entry Date
- Program Exit Date
- Income and Source
- Non-Cash Benefits
- Physical Disability
- Development Disability
- HIV/AIDS
- Substance Abuse
- Domestic Violence
- Destination
- Housing Status
- Chronic Health Condition

Continued on next page

Data quality (continued)

Program-Specific Data Elements: Most of the program-specific data elements are required for HUD McKinney Vento programs that are required to submit Annual Progress Reports (APRs). These programs are Shelter Plus Care, the Supportive Housing Program, Section 8 SRO Mod Rehab for the homeless, and HOPWA-funded homeless programs. The required data elements for programs that submit APRs include:

- Services Received
- Non-Cash Benefits
- Income and Sources
- Physical Disability
- Developmental Disability
- HIV/AIDS
- Mental Health Conditions
- Substance Abuse
- Domestic Violence
- Destination
- Reasons for Leaving

The optional program-specific data elements include:

- Employment
- Education
- General Health Status
- Pregnancy Status
- Veteran's Information
- Children's Education

Program Descriptor Data Elements: The CoC must collect program information in the HMIS for all CoC programs within its jurisdiction, regardless of whether the program participates in the HMIS. The general purpose of these requirements is to ensure that the HMIS is the central repository of information about homelessness in the CoC, including information about programs and clients. Program Descriptor data in HMIS ensures that information about each program is available to: 1) Complete required APRs, 2) Complete Quarterly Performance Reports (QPRs), 3) Calculate rates of HMIS participation; and 4) Monitor data quality.

Continued on next page

Data quality (continued)

The Program Descriptor Data Elements are:

- Organization Identifier
- Organization Name
- Program Identifier
- Program Name
- Direct Service Code
- Site Information
- Continuum of Care Number
- Program Type Code
- Bed and Unit Inventory Information
- Target Population A
- Target Population B
- Method for tracking residential program occupancy
- Grantee Identifier

Data Quality Assurance: To ensure HMIS data quality, HMIS System Administrator utilizes a variety of data quality monitoring reports that identify missing universal data elements including program entry and un-exited clients. Program entry and exit dates are validated against paper records from HMIS participating agencies.

Data Standards Revised Notice

The overall standards for HMIS software are presented in the HMIS Data Standards Revised Notice dated March 2010. Copies will be available upon request.

Missing Value Report

The Missing Value Report calculates the percentage of required client-level data elements with null or missing values divided by the total number of client records. The report will also calculate the number of usable values (all values excluding uDon't know" and "Refused" responses) in each required field over any desired time period (e.g., last month, last year). The report will be generated for each program, for different types of programs, and across the entire CoC. The program level reports will cover all applicable universal and program-specific data elements. The CoC reports will be limited to the following universal data elements: Name, Social Security Number, Data of Birth, Ethnicity, Race, Veteran Status, Gender, Disabling Condition, Residence prior to program entry, and Zip code of last permanent address. Percentages will be based on the universe of client records for which the data element is required. For example, percent (%) null for veterans = number of clients with no veteran status recorded/number of adults.

Unduplication Data Quality Report

The Unduplication Data Quality Report will be available to validate unduplication results based on the HMIS Lead Agency's unduplication approach against other possible combinations of fields. The Unduplication Quality Report highlights records that match, using the HMIS Lead Agency's primary methodology but have conflicting values in other identifiable fields.

Continued on next page

Bed Utilization Report

The Bed Utilization Report will calculate for each program the percentage of beds and family units that are filled on any given night for each program, by dividing the number of clients/households served by the total number of beds/units available for occupancy during the specified time period, as well as the average bed and unit utilization rates by program type. The report will help to identify potential data quality issues by flagging facilities with bed or family unit utilization rates above 105% or below 60%. The report requires that client level data as well as Program Descriptor data be entered into HMIS for all clients served in programs that provide beds.

Data Timeliness Report

This report calculates the differences between the date on which the Program Entry Date or Program Exit Date was entered on clients and the dates on which actual entry or exit occurred for all programs. The report will be based on Program Entry Dates and Program Exit Dates, and compares the dates this data was entered to the actual values contained in those fields. The "Creation Date" for these fields is automatically recorded when the user enters data. This data will be compared to the Data Timeliness Benchmark set by the CoC.

Reduce duplications in HMIS for every HMIS participating agency

In order to reduce the duplication of client records, HMIS participating agency users should:

- Always search for the client in HMIS before creating a new client record.
- Avoid using the 'Anonymous' button unless you are a Domestic Violence Shelter who has an agreement to use this feature.

The burden of not creating duplicate records falls on each participating agency. The HMIS system does not prevent duplicate client records from entering the database, therefore it is up to each user to ensure every client is first searched for, and if not found, then added. If duplicate matches are found, the user must determine if any of the records found, match their client. Having multiple (duplicate) records on the database for a single client causes confusion and inaccurate information being stored and for this the users are discouraged from using Anonymous Client feature. When an HMIS participating agency user is collecting data from a client, the HMIS participating agency user will first attempt to locate that client on the system by searching (Add/Find Client button) by either name (first. last, and middle), Date of Birth (DOB), or Social Security Number (SSN).

It may be possible that a person already exists, but chose to have just his/her client identification number (I.D) Personal Identification Number (PIN) recorded instead of his/her name, SSN, and DOB. It may be required to look in the paper files to determine the client I.D number PIN. If no matches are found on the database for the client, the HMIS participating agency user will continue to add the basic Universal Data elements for the client's intake.

Perform more than one type of search when attempting to find an existing record. Clients often do not use the exact same name that was previously entered. Using a field other than name tends to be more accurate, and not open for much interpretation (DOB, SSN).

Continued on next page

Data quality and correction

Agency Administrators are required to run the Universal Data Quality Report and the Clients in Programs Report for each of the agency's programs and respond to the HMIS Lead Agency's request for data clean-up.

To produce high quality reliable reports, it is imperative to possess high quality data. HMIS Project Managers will help assure stakeholders that the data contained within HMIS is of high quality. Details of the Data Quality Report can be found in the HMIS Quality Plan. At the end of each month, the HMIS System Administrator will review the quality of each agency's data by running reports out of HMIS. The HMIS Committee will then distribute to each agency's Executive Director and Site Administrator a scorecard of the results based on their agency's data. Agency Administrators are required to work with the HMIS System Administrator to rectify any shortfalls in data quality and to fix issues within five business days.

Data use by SBC CoC

Explanation: For the purposes of CoC planning, the aggregate data can be used to generate an unduplicated count of clients and to understand their characteristics, factors contributing to homelessness, and use of system resources. The information can identify gaps and duplication in services.

Data use by OHS

Explanation: For the purposes of system administration, user support, and program compliance, OHS will use the data contained within SBC CoC HMIS for analytical purposes only and will not disseminate client-level data. OHS will release aggregate data contained within SBC CoC HMIS for research and reporting purposes only.

Data use by agency

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 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 HMIS to assist families and individuals to resolve their housing crisis. Proper user training, adherence to SBC CoC HMIS Policies and Procedures, and a clear understanding of client confidentiality are vital to achieving these goals. Any individual or Participating Agency misusing, or attempting to misuse SBC CoC HMIS will be denied access to the system.

Continued on next page

Data use by referral agencies

Referral agencies granted access to the SSC CoC HMIS agree to abide by all applicable laws, and SSG CoC HMIS Policies and Procedures pertaining to client confidentiality, user conduct, security, and the ongoing functionality and stability of services and equipment used to support the SBC CoC HMIS.

The Referral agency users will be given Client Referral access only. This access will allow the user to locate clients at the intake level and then create a referral to a service.

Referral agencies agree not to release client identifiable information to any other organization pursuant to federal and California state law without proper client consent.

Data use by vendor

Explanation: The Vendor and its authorized subcontractor(s) shall not use or disseminate data contained within SSC CoC HMIS without express written permission. If permission is granted, it will only be used in the context of interpreting data for research and for system troubleshooting purposes.

Maintenance of onsite computer equipment

Explanation: Participating Agencies commit to a reasonable program of data 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.

The Executive Management or designee will be responsible for the on-site computer equipment and data used for participation in SSC CoC HMIS including the following:

Computer Equipment: The Participating Agency is responsible for maintenance of onsite computer equipment. This includes the following:

- Workstation(s) accessing SBC CoC HMIS must have a username/ password to log onto Microsoft Windows Operating System.
- Workstation(s) accessing SBC CoC HMIS must have locking, password- protected screen saver.
- Workstation(s) accessing SBC CoC HMIS must have a PKI (Public Key Infrastructure) certificate.
- Workstation(s) accessing SBC CoG HMIS must have a static IP address.
- All workstations and computer hardware (including agency network equipment) must be stored in a secure location (locked office area).

- **Data Storage**: The Participating Agency agrees to only download and store data in a secure environment.
- **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.

Continued on next page

Downloading of data

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

Explanation: To ensure that SBC CoC HMIS is a confidential and secure environment, data extracted from SBC CoC 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 e-mail.

Data sharing

Basic client information within the system will be shared based upon the level of consent designated by the client within SBC CoC 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. Basic client information in the Central Intake includes:

- Demographics
- Household
- Referral
- Eligibility
- Education/Employment
- Scanned Documents

Clients have the ability to agree to the level of consent and time period to which the consent is valid. Participating Agencies are not required to agree to such requested restrictions if collection and sharing of such data is necessary for service delivery and reporting or to consent that is broader than that normally extended at their agency. Clients may elect to share additional information as indicated on the Interagency **Data Sharing Agreement form**.

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, such as:

- Shelter stays
- Food
- Clothing
- Transportation
- Employment
- Housing
- Childcare
- TB clearance status
- Utilities assistance
- Life-skills sessions

Continued on next page

Encryption management

Client Protected Personal Information (PPI) stored on the central server will always be encrypted, except during specific procedures.

Explanation: Client's confidential information will only be decrypted when the San Bernardino County Continuum of Care (SBC CoC) Homeless Management Information System (HMIS) server becomes obsolete and necessitates an upgrade in technology. Should the necessity arise, the HMIS System Administrator, on behalf of the vendor, will obtain the written permission of the Executive Management of each Participating Agency to perform the decryption and subsequent database conversion to a new technology.

Virus protection

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

Explanation: All Participating Agency computers must be protected by anti-virus software. The anti- virus software should be updated regularly to maintain maximum protection from the most recently released viruses. In addition, Agency Administrators should update and install the latest security patches for their operating system which are available from the manufacturer.

Vendor Responsibilities: The vendor will take all necessary precautions to prevent any destructive or malicious program (virus) from being introduced to SBC CoC HMIS. Data and application server will be scanned daily for viruses.

Explanation: The vendor will ensure the following:

- Antivirus software (i.e.: Norton Anti-Virus) and live update scheduled daily.
- Real-time virus scan enabled.

Backup and recovery procedures

SBC CoC HMIS has arranged for regularly scheduled backups of the HMIS database to prevent the loss of data.

Explanation: Multiple levels of backup and storage will be used for key data and files within SBC CoC HMIS. Backups will provide for the loss of multiple cycles.

The vendor will perform data backup procedures in the following manner:

- Daily – resulting in a seven (7) day backup;
- Weekly- resulting in a four (4) or five (5) week backup; and
- Monthly- during the term of contract with the vendor.

Continued on next page

Backup and recovery procedures (continued)

The vendor will maintain an off-site replicate system, which includes off-site storage of tapes in fireproof containers. Back-up tapes that are awaiting delivery to an off-site storage location shall be stored in a fireproof container. The vendor will maintain a one year archive of backups.

The vendor's recovery procedures will be undertaken on a best efforts basis to achieve the following response time:

- Database Loss: Confirmation response and recovery implementation within four (4) hours of reported data loss by client.
- Source code corruption and/ or Loss: Confirmation response within four (4) hours and full initiation of recovery procedures within 24 business hours of reported disruption by client.
- Domain Server Loss: Confirmation response within four (4) hours and full initiation of recovery procedures within 24 business hours of reported disruption by client.
- Database Server Loss: Confirmation response within four (4) hours and full initiation of recovery procedures within 24 business hours of reported disruption by client.
- Disaster: Notification within twenty-four (24) hours and recovery implementation to fully re-establish operations within five (5) business days.

Hosting

SBC CoC HMIS servers will be hosted off-site by the vendor. The vendor will ensure the following: Provides for the provisioning of a secure environment, Internet connection, resilient power supply and the appropriate control mechanism for a customer's application provided by Third party. It includes continuous Network monitoring and diagnostic actions to confirm that the Managed Servers are responding to prescribed standards.

Vendor will:

- Provide a server and rack space for ASP solution.
- Provide a 10/100/1OOOMbps Network connection on a Vendor's switch.
- Provide power (UPS) to the hosted equipment.
- Hosting provider's goal is to maintain 98.4% Server availability
- Cisco routers with advanced port blocking including:
  - Switches with integrated IP blocking based on routine security audit results.
  - System Software Integrated Security.
  - High performance firewall.

The vendor partner is Microsoft Solution Provider and applies security updates at the direction of the vendor.

Continued on next page

Access privileges

Explanation: At the local administrative level each user account can be setup to require a single IP address or multiple addresses in addition to a password to complete a login process. Currently, the system supports one IP address for each user account.

Security monitoring

Agencies will undergo an HMIS security monitoring one year from their implementation date. Each agency is given at time of training guidelines for providing a secure environment for their clients and employees who utilize HMIS. It has been determined that one year after an agency has implemented HMIS is a sufficient amount of time for all issues to be identified and rectified. At the one year mark, Department of Public Social Services (DPSS) will conduct and monitor a security audit at the agency's location.

The following five areas of security will be examined and documented:

1) Physical and Environmental Security:
   a. Personal Computer (PC) location out of public area
   b. Printer location
   c. PC access
2) Personnel Security:
   a. Passwords
   b. Signed Agreements
   c. Number of authorized users
   d. Training provided when needed
3) Application Program and Usage Security:
   a. Printing
   b. Browser Security
   c. Screen Savers
   d. Warnings
   e. Inactivity lock-outs
4) PC Configuration:
   a. Operating System (OS) Version
   b. Browser Configuration
   c. Browser Version
   d. Patch/Update levels current
   e. Virus Protection with updates
   f. Firewall?
5) Network Configuration
   a. Internet Access Method
   b. Firewall/router
   c. Other network users
   d. No Network

Continued on next page

Security monitoring (continued)

The HMIS Project Manager will notify the agency's Executive Director and/or Agency Administrator of an upcoming monitoring. The monitoring will be scheduled in advance, and there will be unannounced HMIS security monitoring visits. The HMIS Project Manager will perform the monitoring and create a results report. This report will be submitted to the agency's Executive Director, the HMIS Committee, and a copy will be filed at the HMIS Lead Agency. Any deficiencies in practices or security must be resolved immediately. A follow-up security audit will be conducted to ensure that the changes have taken affect.

In order to maintain a high level of security, client privacy, and confidentiality practices set-up in this policies and procedures document, security audits will be conducted by HMIS Project Manager on a regular basis. Agency Administrators will work with the HMIS Project Manager to schedule an audit and to assist the HMIS Project Manager in performing the audit. Details of the audit can also be found in the HMIS Quality Plan.
The audit will cover the following topics:

- Informed Consent Agreement,
- Privacy notices,
- Technology security, and
- Data entry practices.

Acknowledgement

I acknowledge that I have received a written copy of the San Bernardino County Continuum of Care (SBC CoC) Homeless Management Information System (HMIS) Policies and Procedures Manual. I understand the terms of SBC CoC HMIS Policies and Procedures and I agree to abide by them.

Agency Name: _____

Printed Name: _____

Signature: _____

Date: _____