

Maricopa HMIS Project
Report on HUD Data and Technical Standards
November 18, 2004

The HUD HMIS Data and Technical Standards were published in the federal Register on July 30, 2004. At the August User Group Meeting, a committee was formed to look at the Data and Technical Standards and to identify the additional requirements to the Continuum of Care, the HMIS Project and to individual agencies that use HMIS.

The committee consisted of:

- Laura Skotnicki, Save the Family
- Justin Graham, Chrysalis Shelter
- Joshua Oehler, HomeBase Youth Services
- Gregg Donnell, Symmetric Solutions
- John Oviatt, Symmetric Solutions
- Robert Duvall, Community Information & Referral

The Data and Technical Standards do not prescribe a methodology for obtaining the data, as long as the definitions of the data elements are used to collect client information. This allows housing and service providers the flexibility to collect the required information in ways that are suitable for the operation of their programs and their local circumstances.

The Data and Technical Standard includes a definition of each data element and required response categories, but does not mandate the procedures for collecting the information. The required response categories can be disaggregated to meet local information needs, as long as the locally-developed response categories can be aggregated to the response categories for each data element in the Data and Technical Standards.

Local providers will be required to report client-level data to a CoC's central data storage facility on a regular basis, sharing of HMIS data among providers within the CoC is not required by HUD and is at the discretion of each CoC and its providers. HUD encourages data sharing among providers within a Continuum of Care as sharing of HMIS information allows maximum benefits from such systems. From an operational perspective, it improves the ability of service provider staff to coordinate and deliver services to homeless clients.

The HMIS initiative is not a federal effort to track homeless people and their identifying information beyond the local level. HUD has no plans to develop a national client-level database with personal identifiers of homeless service users, Any research on the nature and patterns of homelessness that uses client-level HMIS data will take place only on the basis of specific agreements between researchers and the entity that administers the HMIS.

I. Participation

All recipients of HUD funding for homeless activities are required to participate in HMIS. The list of funding sources includes:

- ESG
- SHP
- S+C
- Section 8 SRO
- HOPWA
- CDBG
- HOME

Maricopa HMIS Project
Report on HUD Data and Technical Standards
November 18, 2004

In addition the following other federal programs are included in participation:

- Emergency Food and Shelter (FEMA)
- Runaway and Homeless Youth (HHS)
- Projects for Assistance in Transition from Homeless (PATH) (HHS)
- Transitional Living for Homeless Youth (HHS)
- Family Violence Prevention and Services (HHS)
- Health Center Grants for Homeless Persons (Health Care for the Homeless) (HHS)
- Violence Against Women Grants (DOJ)
- VA Homeless Providers Grants and Per Diem

The 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 regardless of whether they receive funding through the McKinney-Vento Act or from other sources.

The second priority is providers of permanent supportive housing funded by HUD McKinney-Vento Act programs and other HUD programs including HOME.

The third priority is homelessness prevention programs, Supportive Services Only programs funded through HUD’s Supportive Housing Program, and non-federally funded permanent housing programs.

HUD will permit CoCs to stage the entry of domestic violence programs last.

II. Universal Data Elements

All providers participating in a local HMIS will be required to collect the universal data elements from all homeless clients seeking housing or services, including date of birth, race, ethnicity, gender, veteran’s status and Social Security Number (SSN). In addition to personal identifying information, the universal data elements include information on a client’s demographic characteristics and recent residential history in order to enable local providers and communities to analyze patterns of homelessness and service use. Among other important uses, these data will enable CoCs to identify the chronically homeless.

All identifying information, including data elements 2.1 (Name), 2.2 (SSN), 2.3 (Date of Birth), 2.9 (Zip Code of Last Permanent Address), 2.10 Program Entry Date, 2.11 (Program Exit Date), 2.12 (Unique Person Identification Number), and 2.13 (Program Identification Number) need to have special protections to ensure the data are unusable by casual viewers.

| | | | |
|-----|------------------------|-----------------------------------|---|
| 2.1 | Name | First Middle Last Suffix | in SP initial only in SP not in SP |
| 2.2 | Social Security Number | SSN SSN Data Quality Code | in SP not in SP |

| |
|---|
| Maricopa HMIS Project Report on HUD Data and Technical Standards November 18, 2004 |
|---|

| | | | |
|------|-------------------------------------|-----------------------|-----------|
| 2.3 | Date of Birth | Mo/Da/Yr | in SP |
| 2.4 | Ethnicity and Race | Ethnicity | in SP |
| | | Race | in SP |
| 2.5 | Gender | Male/Female Only | in SP |
| 2.6 | Veteran Status | Yes/No | in SP |
| 2.7 | Disabling Condition | Yes/No | not in SP |
| 2.8 | Residence Prior to Program Entry | Type of Residence | in SP |
| | | Length of Stay | not in SP |
| 2.9 | Zip Code of Last Permanent Address | 5 Digit Zip | in SP |
| | | Zip Code Quality Code | not in SP |
| 2.10 | Program Entry Date | Mo/Da/Yr | in SP |
| 2.11 | Program Exit Date | Mo/Da/Yr | in SP |
| 2.12 | Unique Person Identification Number | Computer Generated | in SP |
| 2.13 | Program Identification Number | Computer Generated | in SP |
| 2.14 | Household Identification Number | Computer Generated | in SP |

III. Program Level Data Elements

Program-specific data elements should be collected from all clients served by programs that are required to report this information to HUD or other organizations. Exceptions to this requirement may occur in outreach programs to the street homeless or other nonresidential-based services such as soup kitchens. In such cases, an intake is often not taken, or even possible, and no information is required to access the service.

| | | | |
|------|--------------------------|------------------------------|-----------|
| 3.1 | Income and Sources | Multiple Sources and Amounts | in SP |
| 3.2 | Non-Cash Benefits | Multiple Listings | in SP |
| 3.3 | Physical Disability | Yes/No | not in SP |
| 3.4 | Developmental Disability | Yes/No | not in SP |
| 3.5 | HIV/AIDS | Yes/No | not in SP |
| 3.6 | Mental Health | Yes/No | not in SP |
| | Long Term | Yes/No | not in SP |
| 3.7 | Substance Abuse | Alcohol/Drug/Dual | not in SP |
| | Long Term | Yes/No | not in SP |
| 3.8 | Domestic Violence Victim | Yes/No | in SP |
| | If Yes When | 3 mo/6 mo/1 yr/ more | not in SP |
| 3.9 | Services Received | Mo/Da/Yr | in SP |
| | Service Type | Drop down or AIRS Taxonomy | in SP |
| 3.10 | Destination | Drop down box | in SP |
| | Tenure | Drop down box | not in SP |
| | Subsidy Type | Drop down box | not in SP |
| 3.11 | Reasons for Leaving | Drop down box | in SP |
| 3.12 | Employment | Yes/No | not in SP |
| | If working hr last week | No. of Hours | not in SP |
| | Tenure | Perm/Temp/Seasonal | not in SP |
| | Is client looks for work | Yes/No | not in SP |

| |
|--|
| <p>Maricopa HMIS Project Report on HUD Data and Technical Standards November 18, 2004</p> |
|--|

| | | | |
|------|------------------------------|------------------|-----------|
| 3.13 | Education currently enrolled | Yes/No | not in SP |
| | Receiving Voc. Training | Yes/No | not in SP |
| | Highest Level Completed | Drop down box | in SP |
| | What Degrees Held | Multiple Answers | not in SP |
| 3.14 | General Health Status | Drop down box | not in SP |
| 3.15 | Pregnancy Status | Yes/No | in SP |
| | If yes, Due Date | Mo/Da/Yr | in SP |
| 3.16 | Veteran's Information | | |

If Client answered yes to veteran status on universal data elements then they must answer seven questions for every military service era that is identified.

| | | |
|--------------------------|---------------|-----------|
| Military Service Eras | Drop down box | in SP |
| Duration of Duty | No. of months | not in SP |
| Served in war zone | Yes/No | in SP |
| If yes, name of war zone | Drop down box | in SP |
| If yes, no. of months | No. of months | not in SP |
| If yes, received fire | Yes/No | not in SP |
| Branch of Military | Drop down box | in SP |
| Discharge Status | Drop down box | in SP |

For children between 5 and 17 years old the following five questions must be answered:

| | | | |
|------|---------------------------|----------------|-----------|
| 3.17 | Children's Education | | |
| | Current Enrollment Status | Yes/No | in SP |
| | If yes, name of school | Text | in SP |
| | If yes, type of school | Public/Private | not in SP |
| | In no, Last enrolled | Mo/Yr | not in SP |
| | If no, problem enrolling | Drop down box | not in SP |

IV. Privacy Standards

The privacy standards apply to all organizations involved in the HMIS Project. Each agency must examine the requirements in this section to ensure that the agency is in compliance.

Protected Personal Information (PPI) is any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that:

- Identifies, either directly or indirectly, a specific individual;
- Can be manipulated by a reasonably foreseeable method to identify a specific individual;
- or
- Can be linked with other available information to identify a specific individual.

Covered Homeless Organization (CHO) is any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PPI on homeless clients for an HMIS.

Any CHO that is covered under the HIPAA is not required to comply with the privacy or security standards in the HUD standards if the CHO determines that a substantial portion of its

Maricopa HMIS Project
Report on HUD Data and Technical Standards
November 18, 2004

PPI about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules.

The HMIS standards give precedence to the HIPAA privacy and security rules because: (1) The HIPAA rules are more finely attuned to the requirements of the health care system; (2) the HIPAA rules provide important privacy and security protections for protected health information; and (3) requiring a homeless provider to comply with or reconcile two sets of rules would be an unreasonable burden.

A CHO may use or disclose PPI from an HMIS under the following circumstances:

- To provide or coordinate services to an individual;
- For functions related to payment or reimbursement for services;
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or
- For creating de-identified PPI.

Under the HMIS privacy standard, these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards).

- Uses and disclosures required by law.
- Uses and disclosures to avert a serious threat to health or safety.
- Uses and disclosures about victims of abuse, neglect or domestic violence.
- Uses and disclosures for academic research purposes.
- Disclosures for law enforcement purposes.

All CHOs must comply with the baseline privacy requirements described here with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO may adopt additional substantive and procedural privacy protections that exceed the baseline requirements for each of these areas.

A CHO must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the individual. A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. Consent of the individual for data collection may be inferred from the circumstances of the collection.

A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to: (1) Restricting collection of personal data, other than required HMIS data elements; (2) Collecting PPI only with the express knowledge or consent of the individual (unless required by law); and (3) Obtaining oral or written consent from the individual for the collection of personal information from the individual or from a third party.

PPI collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PPI should be accurate, complete and timely.

A CHO must develop and implement a plan to dispose of or, alternatively, to remove identifiers from; PPI that is not in current use seven years after the PPI was created or last changed.

Maricopa HMIS Project
Report on HUD Data and Technical Standards
November 18, 2004

A CHO must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures.

A CHO must publish a privacy notice describing its policies and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page. A CHO may, if appropriate, omit its street address from its privacy notice. A CHO must post a sign stating the availability of its privacy notice to any individual who requests a copy.

A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change.

In general, a CHO must allow an individual to inspect and to have a copy of any PPI about the individual. A CHO must offer to explain any information that the individual may not understand.

A CHO must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual.

A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

V. Security Standards

All CHOs must comply with the security requirements.

A CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes and servers.

A CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

- Using at least one number and one letter;
- Not using, or including, the username, the HMIS name, or the HMIS vendor's name; and/or
- Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Maricopa HMIS Project
Report on HUD Data and Technical Standards
November 18, 2004

Written information specifically pertaining to user access (*e.g.*, username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

A CHO must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are Accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall as long as the server has a firewall.

HMIS that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates or extranets that limit access based on the Internet Provider (IP) address, or similar means.

A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times.

A CHO must copy all HMIS data on a regular basis to another medium (*e.g.*, tape) and store it in a secure off-site location where the required privacy and security standards would also apply. A CHO that stores data in a central server, mini-computer or mainframe must store the central server, mini-computer or mainframe in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors must be used to protect systems used for collecting and storing all the HMIS data.

In order to delete all HMIS data from a data storage medium, a covered homeless organization must reformat the storage medium.

A CHO must use appropriate methods to monitor security systems. Systems that have access to any HMIS data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely.

A CHO must apply application security provisions to the software during data entry, storage and review or any other processing function. A CHO must secure all electronic HMIS data with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Maricopa HMIS Project
Report on HUD Data and Technical Standards
November 18, 2004

A CHO must encrypt all HMIS data that are electronically transmitted over the Internet, publicly accessible networks or phone lines to current industry standards. The current standard is 128-bit encryption.

A CHO must store all HMIS data in a binary, not text, format. A CHO that uses one of several common applications (*e.g.*, Microsoft Access, Microsoft SQL Server and Oracle) are already storing data in binary format and no other steps need to be taken.

A CHO must secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms.

A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.

VI. Technical Standards

Any HMIS application must be capable of exporting any and all data collected into a comma-separated values text file using the following format:

- All fields in a given record are separated by a comma;
- All records within a given text file contain the same fields;
- Blank fields are signified by the comma ending the previous field (or the beginning of the line if the field is the first in the record) followed by a comma indicating the end of the empty field;
- Fields containing text information (as opposed to numeric) will be surrounded by double quotes whenever the field includes blank spaces, commas, or other symbols not part of the standard alphabet;
- The first line of the file shall be a list of the field names included in every record in the file; and
- The list of field names shall be in the same format described above.

The CoC must have or designate a central coordinating body that will be responsible for centralized collection and storage of HMIS data.

HMIS data must be collected to a central location at least once a year from all HMIS users within the CoC.

HMIS data must be stored at the central location for a minimum of seven years after the date of collection by the central coordinating body or designee of the CoC.