Metropolitan Denver Homeless Initiative

Homeless Management Information System

Policies & Procedures

Administered By:

Table of Contents

1. Colorado HMIS Historical Background

1.1 Definition of Homeless Management Information System

An HMIS is a computerized data collection tool used by communities to collect ongoing data on persons who are homeless or receive assistance from the community. This longitudinal data can be used to accurately calculate the size and needs of these populations.

1.2 HUD HMIS Requirement

In July 2003, the Department of Housing and Urban Development (HUD) published a draft notice of an HMIS. By July 2004, HUD finalized the requirements for HMIS. Both notices prompted communities around the nation to set up an HMIS program to capture the requested information. The notices specified what pieces of data to collect as well as establishing minimum baseline policies and procedures that communities must follow when operating their HMIS. An Annual Homeless Assessment Report (AHAR) report will be requested of each continuum starting in 2005. Additionally, the SuperNOFA grant application rates each continuum's progress in its HMIS implementation. Therefore, as more agencies and programs participate in HMIS, the stronger our community's SuperNOFA grant application is for the available funds.

1.3 Vision for HMIS

Different versions of HMIS existed in Colorado many years before HUD required HMIS implementation. The goals and overall vision for HMIS within our state exceeds HUD's reporting requirements. Clients, agencies, and the community benefits from HMIS participation. Clients will experience a streamlined process of referrals, intake, and assessment across the entire service delivery experience. If clients desire, they can receive coordinated case management across different agencies, programs, and services such that they have one coordinated plan to fulfill. Agencies will be able to track and measure outcomes of their programs. They will be able to coordinate services better internally as well as externally. Agencies will have more information to share with funders, boards, and other stakeholders. The community benefits as well by understanding at a higher level what the problems, issues, and needs are most concentrated. Policies can be developed or modified to reduce identified service gaps. The functionality contained within HMIS will enable all of these things to happen, as HMIS evolves for our community.

2. Colorado HMIS Structure

2.1 Continuums of Care

The state of Colorado is organized into three geographically-based Continuums of Care (CoC). Each CoC is responsible for working with homeless assistance agencies in their geographic area to coordinate the delivery of housing and services to homeless families, individuals, youth, and persons with disabilities. Additionally, the CoCs are responsible for implementing and managing HMIS within their community. The three CoCs in Colorado are:

- Metropolitan Denver Homeless Initiative (MDHI) – seven county area (Adams, Arapahoe, Boulder, Broomfield, Denver, Douglas, and Jefferson)
- Homeward Pikes Peak (HPP) – El Paso county
- Balance of State (BoS) – remainder of Colorado

All three CoCs from Colorado have joined together to utilize the same HMIS solution, policies and procedures such that HMIS operations are standard throughout Colorado.

2.2 HMIS Solution

The vendor supplying the HMIS solution is VisionLink, Inc. Located in Boulder, VisionLink provides database management solutions nationally. Its Tapestry module within the CommunityOS solution, handles 2-1-1 operations as well as HMIS. VisionLink is responsible for:

- Providing Colorado's Internet-based 2-1-1/HMIS
- 211 & HMIS software upgrades
- Hosting (maintaining, securing, performing backups, and ensuring availability) of Colorado's HMIS
- Providing training and technical support to HMIS Administrators

More information on VisionLink can be found at: www.visionlink.org

2.3 Mile High United Way

Mile High United Way (MHUW) has entered into a contract with VisionLink for use of Tapestry. Under this agreement, MHUW is licensed to use Tapestry with the right to further sub-license it to make the system available to its agency partners and the service providers they represent. User sub-licenses for Colorado HMIS are available at no charge to agencies. In this agreement, MHUW is generally responsible for:

- Performing all System Operator functions for 2-1-1
- Providing oversight to HMIS system operations
- Ensuring the joint 2-1-1/HMIS solution, policies & procedures, and system administration are agreeable for all Tapestry partners in Colorado.

2.4 Colorado Department of Human Services, Supportive Housing & Homeless Programs

Under the MHUW contract with VisionLink, the CDHS-SHHP office provides the HMIS implementation and program management on behalf of the MDHI CoC. SHHP works with various MDHI committees to coordinate the overall HMIS effort for the seven county metro Denver area. As the HMIS Administrator, SHHP is responsible for many activities including:

- Chairing the HMIS Users Group
- Preparing agencies within the CoC for implementing Tapestry
- Defining policies and procedures within the federal guidelines, best practices, and MDHI members' input
- Advocating HMIS software enhancements on behalf of partner agencies
- Initial and on-going training for HMIS
- Providing quality assurance for the HMIS program
- Fulfilling CoC reporting requirements on behalf of the MDHI
- Operating the MDHI HMIS Helpdesk

2.5 Participating Agencies

Under the MHUW 2-1-1/HMIS license for Tapestry, any agency may participate in HMIS if they have signed the Agency User Agreement and agree to abide by the policies and procedures outlined in this document. Each participating agency owns and is responsible for its clients' data. All types of agencies that provide services to persons in need are eligible.

2.6 Users

Users are authorized by their agency's Executive Director or other persons within the agency having the appropriate authority. Users are allowed to use HMIS after signing an End User Agreement with their agency, and completing the necessary training. Users are responsible for following the policies and procedures outlined in this document, and are ultimately responsible for collecting and entering client data.

2.7 HMIS Users Group

The purpose of the HMIS Users Group is to bring together participating agencies' HMIS users to share information and make recommendations on a number of factors regarding HMIS. It is a forum for sharing best practices among agencies, as well as a way to suggestion improvements in policies and procedures. Future enhancements to HMIS will also be discussed during these meetings. It is expected that participating agencies send at least one person to every HMIS users group.

Policy: MDHI HMIS User Group meetings held every third Thursday from 2pm - 4pm.

Effective Date: *June 22, 2006*

2.8 Clients

Clients choose to participate in HMIS with written authorization to allow an agency's users to collect and enter their personal information into HMIS. It is extremely important in the use of HMIS that client confidentiality, privacy, and security are maintained at a very high level. The policies and procedures written in this document fulfill basic HUD HMIS requirements, utilize best practices for the industry, and are further enhanced for our community.

3. Implementing HMIS

3.1 Agency Partnership Agreement

Policy: To participate in HMIS, an agency must sign and agree to abide by the terms of the Agency Agreement.

Effective Date: *May 10th, 2005*

Description:

The Agency Agreement is a contract between the agency and the HMIS Administrators (CDHS-SHHP) regarding participation in HMIS using the Tapestry software. The agreement outlines specific requirements on confidentiality, data entry, responsibilities, security, reporting, and other items deemed necessary for proper HMIS operation.

Procedures:

1.The agency's Executive Director (or other empowered officer) will sign 2 copies of the Agency Agreement, and mail them to:

Attn: Colorado HMIS

Colorado Department of Human Services

Supportive Housing & Homeless Programs

4020 S. Newton Street

Denver, CO 80236

2.Upon receipt of the signed agreement, it will be signed by SHHP's Executive Director. One copy will be filed at SHHP; the other copy will be mailed back to the agency.

3.Any questions regarding the terms of the Agency Agreement should be directed to the Colorado HMIS Helpdesk.

3.2 Designate Agency Site Administrator

Policy: The agency's Executive Director or other empowered officer must designate an individual to act as the agency's Site Administrator role.

Effective Date: *May 10th, 2005*

Description:

The Site Administrator role at an agency possesses different responsibilities than a typical End User. The Site Administrator is accountable for the following items:

- Maintain the agency, programs, and services profiles in Tapestry

- Communicate personnel/security changes for HMIS users
- Act as the first tier of support for HMIS users
- Act as the main point of contact for HMIS System Administrators
- Ensure client privacy, confidentiality, and security
- Maintain compliance with technical requirements for participation
- Store and enforce End User Agreements
- Post Privacy Notice
- Enforce data collection, entry, and quality standards
- Assist HMIS System Administrators with On-Site Technical Assistance/Audits
- Attending the HMIS Users Group

Procedures:

1.The Agency Agreement must be signed and returned.

2.The Executive Director or other empowered officer will contact the Colorado HMIS helpdesk to notify them which person will act as the Site Administrator.

3.This individual must sign the End User Agreement with the agency, stating that they understand what is required of them for HMIS.

4.This individual must attend the HMIS Site Administrator training course before gaining access to HMIS and Site Administrator privileges. Read the section on Training to learn how to attend a class.

Best Practices:

1.Depending upon your agency's organization, consider designating a second Site Administrator to act as a backup.

2.If your organization would like to designate multiple Site Administrators, contact the HMIS System Administrators first.

3.3 Technological Requirements for Participation

Policy: All computers authorized to access Colorado HMIS must meet the minimum requirements as established in this manual.

Effective Date: *May 10th, 2005*

Procedures:

All computers that will access Colorado HMIS on behalf of the agency must meet the minimum requirements. This includes agency's on-site desktops, laptops, as well as home computers. Accessing HMIS from home is allowed, though this practice is strongly discouraged because of security concerns. From an agency's viewpoint, it is difficult to ensure that a computer in the home meets the technical standards and that users are abiding by the same privacy, confidentiality, and security procedures as they would in the office. Unauthorized individuals (spouses, children, relatives) could gain access to HMIS in a home environment more easily than in an office environment. Site Administrators must ensure that these computers meet the following standards:

1.Internet access: Any computer that will be used for HMIS must be able to connect to the Internet for the purpose of accessing the HMIS software, as long as it is not AOL.

2.Internet browser software: The browser must be capable of 128-bit encryption.

3.Internet connection speed: If you are using dial-up connection to get to the Internet, the minimum speed is 33.6 kbs (33,600 bytes/second).

4.Hardware processor: The PC speed should be at least 350 MHz.

5.Hardware RAM memory: The PC should have at least 64MB RAM.

6.Screen resolution: Screen resolution should be at least 800 x 600.

7.Firewall: For your computer or network, an active firewall must be present either on that PC or as a part of the network.

8.Virus protection: For your computer or network, virus protection software must be present and active, with current virus definitions.

9.Login access: Each computer must utilize and activate a login screen.

10.Screen-saver password: Each computer must activate a screen-saver password which is set to turn on when the computer is unattended or has not been in use during a reasonable amount of time (around 10 minutes).

Best Practices:

Agencies should also include these recommendations in preparation for fully utilizing all the capabilities within HMIS, as well as incorporating standard industry practices:

1.Operating system version: Each computer should be on a currently supported version of an operating system (e.g. Windows, Mac O/S). The oldest version of Windows supported by Microsoft is 98. Windows 98, 98 Second Edition (SE), and Millennium Edition (ME) are going to be supported through June 30, 2006.

2.Operating system updates: Each computer accessing HMIS should be current in applying all of the available critical security patches. Patches should be installed within 24 hours of notification of availability.

3.Anti-Spyware software: For your computer or network, anti-spyware software should be present, active, and with current definitions.

4.Browser software version: Each computer should be on a current version of the browser. Internet Explorer 6.0.2 and Netscape Navigator 7.2 are the most current versions of those browsers.

5.High-speed connection: Ideally each computer should have access to at least a DSL/Broadband high-speed line instead of dial-up connection. This will result in a much improved experience over connecting with dial-up speeds.

6.Standard office software: In order to use downloaded data from HMIS, you should have software that can interpret comma-delimited files, such as spreadsheet, word processing, or database software (examples like Microsoft's Excel, Word and Access). There are a number of options here. It is not a requirement that you have this software since it is not required that you download HMIS data. There are additional options beyond the Microsoft Office software.

7.Compressed file expander: For computers that will download data from HMIS, it will need a compressed file expander to unzip the file. WinZip and Aladdin Expander are of this type of software. It is not a requirement that you have this software unless you intend to download data.

3.4 Complete Agency Profiles in HMIS

Policy: Agencies are not allowed to enter client data into HMIS until their set of profiles has be completed in HMIS and approved by HMIS System Administrators.

Effective Date: *May 10th, 2005*

Description:

Within HMIS, each agency must set up a group of profiles that define the programs and services the agency offers. Most agencies have been exposed to profiles, from the 2-1-1 effort. The HMIS profiles will be similar to the 2-1-1 profiles, but there are differences. Site Administrators will be trained in creating, updating, and maintaining both 2-1-1 and HMIS profiles.

Procedures:

1.The Site Administrator must have successfully attended HMIS Site Administrator training to learn how to set up their agency's profiles in HMIS.

2.The Site Administrator will complete the Profile Worksheet to assist in the organization of how an agency's profiles will work in Tapestry, before updating profiles in Tapestry.

3.The Site Administrator will contact the Colorado HMIS Helpdesk, for the purpose of reviewing the Profile Worksheet.

4.The HMIS System Administrators will work with the Site Administrator to ensure that the profiles are organized in a way that is useful for the agency, consistent with standard practices, and meets reporting needs.

5.The Site Administrator will complete the agency profile set up in Tapestry based on the final Profile Worksheet.

6.When finished, the Site Administrator will contact the Colorado HMIS Helpdesk for the purpose of reviewing the profile set up in Tapestry.

7.The Site Administrator will make any necessary changes to profiles as required by the HMIS System Administrators.

Best Practices:

1.It is strongly recommended that Site Administrators familiarize themselves with the Profile Worksheet before attending HMIS Site Administrator training.

2.HMIS could produce reports that were previously not possible within the agency. Determine what reporting information members would like to have, in addition to what is currently required. Profiles could be set up in HMIS enabling members to get this information.

3.Once client data entry into the agency's profiles begins, it is difficult to make changes to the structure without having to deal with many issues.

3.5 Data Conversion/Data Integration

Policy: Agencies utilizing systems other than CHIRP, are responsible for converting any data that they wish to carry-over into HMIS.

Effective Date: *May 10th, 2005*

Description:

Agencies may already collect client data in another system, whether it is packaged software or homegrown. There may be a desire to carry over information from that system into HMIS. There are two general ways to accomplish this:

1.Data Conversion: This is a one-time transfer of data from the old system into HMIS, and users would actively utilize HMIS after that.

2.Data Integration: This is a regularly, scheduled data transfer from the current system into HMIS (e.g. Monthly data feed), and users would continue to use the agency's system in lieu of HMIS.

Either option is complex with the number of variables involved in performing these tasks. In general there are very specific requirements for conversion and integration. Agencies should contact the Colorado HMIS Helpdesk if they desire to do either one.

Data Conversion Requirements:

1.HMIS Informed Consent must be collected for records that will be converted from one system to the next. Records will not be converted for clients where there is no signed Informed Consent Agreement, because the client will not have agreed to allow their information to be entered into HMIS.

2.Beyond CHIRP users, agencies are required to pay for the cost of data conversion. SHHP will assist in the introductions to VisionLink and Mile High United Way for this activity, but will not take part in pricing or contract negotiations.

Data Integration Requirements:

1.The system that will primarily be used for client-level data must be in full compliance with HMIS standards as directed in the Federal Register.

2.Agencies must still follow the same policies and procedures as other agencies. These policies and procedures protect client privacy, confidentiality, and security.

3.There may be additional costs to the agency to set up data integration into HMIS, as well as on-going costs too.

4.Agencies must be aware that if this option is chosen, they will not have access to the benefits of using 2-1-1 and HMIS. Their clients will not be able to:

- Have their record electronically shared with other agencies to provide them with easier intakes, and faster service delivery
- Participate in the rapid entry, client id with bar code solution
- Receive coordinated case management service across multiple agencies
- Benefit from a community-wide collaboration effort to make service delivery better

3.6 Designating HMIS End Users

Policy: Any individual working on behalf of the agency (employee, contractor, and volunteer), that will collect information for HMIS purposes must be designated an HMIS user; and therefore is subject to these policies and procedures.

Effective Date: *May 10th, 2005*

Description:

Anybody who collects any HMIS data (electronic or paper) or creates reports from the system should be designated as an HMIS user. The reason is that there are client privacy, confidentiality, and security procedures that everyone in those positions must be aware of and follow. Individuals who have not had the proper training will not be equipped to respond to clients' questions on HMIS informed consent, revocation, intake forms, and other aspects. Individuals who are designed HMIS users that will not work with the HMIS software, are required to take the Policies & Procedures training class. Individuals who will work with the HMIS software, will take this class as well as specific training on the HMIS software.

Procedures:

1.After an individual is identified as an HMIS user, the Site Administrator must follow the User Administration procedures in this document for adding authorized users.

2.This individual is required to complete the appropriate user training, as outlined in the Training procedures stated in this document.

Best Practices:

1.It is in the best interest of agencies to designate many people as HMIS users. More people will be able to help answer client's questions and/or concerns.

2.Most agencies will benefit from sending more people to training, as a way of reinforcing current agency policies regarding informed consent, confidentiality, security, etc.

4. User Administration

4.1 Authorizing Personnel for HMIS

Policy: Only authorized individuals that have successfully completed the necessary steps may be allowed to access HMIS on behalf of an agency.

Effective Date: *May 10th, 2005*

Procedures:

1.The Site Administrator will update the agency's Approved Users List spreadsheet to reflect the newly authorized individual, assign the security level, and will submit it to the Colorado HMIS helpdesk.

2.This individual must successfully complete the HMIS Policies & Procedures class.

3.If this individual needs access to the software, they must also complete the appropriate HMIS User Training class.

4.This individual must sign the End User Agreement with the agency, stating that they understand what is required of them for HMIS.

4.2 End User Agreements

Policy: A Colorado HMIS End User Agreement must be signed and kept for all agency personnel or volunteers that will collect or use HMIS data on behalf of the agency.

Effective Date: *May 10th, 2005*

Description:

The End User Agreement is a document between a participating agency and its employees, contractors, or volunteers who are authorized to collect HMIS data and/or record that data into the system, for the purpose of agreeing to abide by the rules in the specified.

Procedures:

1.Before an authorized agency personnel begins collecting data on behalf of HMIS, the individual must sign a current Colorado HMIS End User Agreement form.

2.An agency must store the signed Colorado HMIS End User Agreement for each individual that will collect data for HMIS or will operate the HMIS software.

3.An agency must never dispose of a signed Colorado HMIS End User Agreement upon revoking an individual's authorization or in terminating an individual's employment.

Best Practices:

1.An agency could choose to store all of the Colorado HMIS End User Agreements in one central location or person (like the HMIS Site Administrator) as opposed to storing the document in their employee file. With standard business practice, terminated employees' files tend to get purged after a period of time. Therefore with the need to keep end user agreements indefinitely, it may be easier for an agency to separate this from an individual's files.

2.For new hires, if their position is authorized to collect HMIS data or utilize the HMIS software, the End User Agreement form can be included in their agency orientation procedures.

4.3 Assigning Security Levels

Policy: Agencies will assign users an appropriate security level such that the user only has access to HMIS functionality or information required to successfully fulfill their role.

Effective Date: *May 10th, 2005*

Description:

Within HMIS, each user is assigned a security level based on the tabs they have access to. This security allows user to gain access to certain areas of the HMIS application. This security feature is utilized to ensure that individuals can only access the type of client information they need to do their job within the agency. An example would be that an intake specialist would be assigned security to access the general information page so that they could enter or view a client's demographic information (name, birth date, ethnicity, etc.), however, their security role would not allow them to view any case management notes that may exist. Below is a description of each tab in Tapestry:

•General Information (Universal): basic demographic information like name, birth date, etc. Everyone is granted access to this tab automatically.

•Selected Service (Universal & Program-Specific): enroll and exit in programs, record service delivery

•Homeless Management (Universal & Program-Specific): homeless status, background on their homeless episodes

•Household (Universal): creation of a household by linking together multiple clients

•Income & Benefits (Program-Specific): recording income by different categories, recording non-cash benefits (TANF, food stamps, etc.)

•Education (Program-Specific): adult and children education status, current school and training information

•Military (Program-Specific): detailed information regarding a client's military background, such as branch, current status, geographic area(s) served

•Health (Program-Specific): data on health status, disability status, dependencies, etc.

•Employment (Program-Specific): current job status, employer information

•Domestic Abuse (Program-Specific): domestic violence background information

•Referral (optional feature): needed if the agency would like to make and track referrals to other agencies listed in 2-1-1

•Case Management (optional feature): needed if the agency would like to add general case management notes

•History (optional feature): needed if the agency would like to see all of the types of case management notes together in one tab (pulls from other tabs beyond Case Management)

•Expenses (optional feature): different categories and line items of expenses for budgeting purposes

•Messages (optional feature): allows user to record when email are sent, phone conversations, and/or mail is sent to the client (like contact management)

•Addresses (optional feature): allows user to record various types of additional client addresses (seasonality, temporary, new permanent).

Procedures:

1.An agency must first determine what tabs they are required to complete to fulfill reporting requirements. There are tabs related to being able to enter in the Universal data elements, and a set of tabs related for the Program-specific data elements.

2.The agency must then determine any additional tabs they would like access to beyond their required data collection. For example, an agency that is only required to collect the Universal data elements may decide that they would also like to have the Income and Education tabs too.

3.The Site Administrator is then responsible for granting individuals access to the appropriate tabs based on their role in the organization. An intake specialist could be granted access to all of the tabs to complete the Universal and Program-specific data elements OR just the General Information tab. To assign the security level, the Site Administrator will updated the Approved Users List, and submit that to the Colorado HMIS Helpdesk.

Best Practices:

1.When selecting which tabs an agency wants to use in HMIS, start with the end goal in mind rather than going from what is the least amount of information needed to fulfill reporting requirements. Think about how you currently do business, and how you would like to do business in the future. One might find that HMIS is a conduit for providing additional services to an agency's clients because of its features.

2.There is a strong tendency to grant access to all information to every staff person because it is easier to administer that way. However, it is important to keep with the idea of 'minimal access' or more commonly put 'on a need to know basis'. Grant permissions to areas only where that person will need to add or view data. For example, it is generally not appropriate to grant access to the Case Management tab to a volunteer who is performing basic intake.

4.4 Changing Personnel Security Levels

Policy: Agencies request a security level change for an individual by notifying the Colorado HMIS team.

Effective Date: *May 10th, 2005*

Procedures:

1.The Site Administrator will update the agency's Approved Users List spreadsheet to reflect the newly authorized individual, and will submit it to the Colorado HMIS helpdesk.

2.If the security change is to make them the new Site Administrator, they must first complete the HMIS Site Administrator training before the Colorado HMIS team will change the security.

3.If the security change is to enable them access to the HMIS software, they must first complete the HMIS User training before the Colorado HMIS team will change the security.

4.For other requests, the Colorado HMIS team will respond within 1 business day to the request. Security changes for non-site administrators will take effect immediately.

4.5 Removing Authorized Personnel

Policy: The Colorado HMIS team must be notified within 1 business day when an individual is no longer authorized to access HMIS on the agency's behalf.

Effective Date: *May 10th, 2005*

Procedures:

1.Within 1 business day of revoking an individual's authorization for HMIS access, the agency will contact the Colorado HMIS Helpdesk via email (colorado.hmis@state.co.us) or telephone (303-866-7109).

2.The agency will update their Approved Users List spreadsheet to reflect the change, and if they have not already done so, submit it to the Colorado HMIS Helpdesk.

3.Upon receipt of the request, the Colorado HMIS System Administrator will immediately deactivate the individuals' HMIS user account, which means they can’t login.

5. Training

5.1 Site Administrator Training

Policy: Individuals designated as an agency's site administrator must complete a 1-day HMIS Site Administrator training course before being granted the appropriate security level.

Effective Date: *May 10th, 2005*

Description:

The HMIS Site Administrator training will cover several topics covering the duties and procedures specifically related to the role, beyond a typical End User training session. Topics will include:

- 2-1-1 & HMIS Organization
- HMIS Policies & Procedures
- Client Privacy & Confidentiality
- Tapestry (HMIS) Basics
- Tapestry Administration

Procedures:

1.The agency must have signed and returned the Agency Partnership Agreement before the individual can attend HMIS Site Administrator training.

2.This individual can contact the Colorado HMIS Helpdesk or check online to see when the next training day is being offered, and can RSVP as stated in the directions. Training spots are allocated on a first-come first-serve basis. Typically class sizes are 8-12 individuals.

3.Once the individual completes their training successfully, they will be assigned the appropriate security level at that time.

4.If this individual will also enter client level data, they need to also attend the HMIS End User Training.

5.2 HMIS Policies & Procedures Training

Policy: Individuals who are authorized to collect HMIS information are required to complete a ½ day training regarding HMIS Policies & Procedures.

Effective Date: *May 10th, 2005*

Description:

This class is intended for everyone that will collect data on behalf of HMIS, including intake personnel, volunteers, and case managers for example. The class will cover in detail this policies & procedures as it relates to collecting data, expectations, and other materials. A large topic in this class with is client privacy, confidentiality, and security as it directly relates to HMIS.

Procedures:

1.The agency must have signed and returned the Agency Partnership Agreement before the individual can attend HMIS Policies & Procedures training.

2.This individual can contact the Colorado HMIS Helpdesk or check online to see when the next training day is being offered, and can RSVP as stated in the directions. Training spots are allocated on a first-come first-serve basis.

3.Once the individual completes their training successfully, they will be eligible to attend the HMIS End User training.

5.3 HMIS End User Training

Policy: Individuals who need to enter data in the HMIS software are required to complete a ½ day HMIS User training before being granted access to the software.

Effective Date: *May 10th, 2005*

Description:

The HMIS End User training will cover several topics related to the HMIS program operations. Topics will include:

- 2-1-1 & HMIS Organization
- Tapestry (HMIS) Basics
- Tapestry Data Entry

Procedures:

1.There are several prerequisites for attending the HMIS End User training:

- The agency must have signed and returned the Agency Partnership Agreement before

the individual can attend HMIS End User training.

- The agency must have a designated Site Administrator.
- The agency's profiles must be completed.
- The individual must be authorized on the agency's Authorized Users List.
- The individual must have completed the HMIS Policies & Procedures training.

2.This individual can contact the Colorado HMIS Helpdesk or check online to see when the next training is being offered, and can RSVP as stated in the directions. Training spots are allocated on a first-come first-serve basis. Typically class sizes are 8-12 individuals.

3.Upon completion training, they will register for a login and password at the HMIS Live Site at http://211colorado.communityos.org.

4.The Colorado HMIS team will immediately activate the user and assign appropriate security levels based on the agency's Approved Users List.

5.At this point, the individual is able to work in the HMIS software.

5.4 HMIS Software Upgrade Training

Policy: When new 211/HMIS software functionality is available, additional trainings regarding the upgrade will be offered.

Effective Date: *May 10th, 2005*

Description:

HMIS will evolve over time to include additional capabilities that agencies and the community have requested. While documentation will be sent out for each upgrade, there may be occasions where supplemental training would be the best way for individuals to learn how to use the new capability. The upgrade training will typically be conducted remotely through web or audio conferencing, and would be short.

Procedures:

1.After a new version of HMIS is available, HMIS Administrators will send a notice to all users with any additional, appropriate documentation.

2.If it is determined that supplemental training would be beneficial, the upgrade training schedule would be announced at that time too.

3.To register, individuals will RSVP as stated in the directions. Spots are allocated on a first-come first-serve basis.

Best Practice:

1.The Site Administrator should attend the upgrade training in order to keep up with all the

possibilities in applying all the HMIS functionality at their agency.

2.Agencies should strongly encourage all end users to attend, as new functionality may be introduced to make their jobs easier or allow them to do more with what is available.

5.5 Seminars

Policy: Special topic-based seminars will be offered by the HMIS Administrators on a regular basis.

Effective Date: *May 10th, 2005*

Description:

As HMIS evolves, many agencies will find that they are looking for the same type of information or best practices. As this need is recognized, HMIS Administrators will organize seminars to discuss these special topics.

Procedures:

1.When a special topic seminar is requested or a need is discovered, HMIS Administrators will send a notice to all users.

2.To register, individuals will RSVP as stated in the directions. Spots are allocated on a first-come first-serve basis.

Best Practice:

1.Agencies are strongly encouraged to nominate topics that they feel other agencies would benefit from too. This is especially true if an agency would like to share a best practice.

6. Data Collection Processes

6.1 On Whom To Collect Data

Policy: At a minimum, agencies are required to attempt data collection on individuals who are homeless and are receiving services from the agency.

Effective Date: *May 10th, 2005*

Procedures:

1.For HMIS purposes, HUD's minimum standards require that individuals who are homeless and receive services from an agency must be approached for HMIS data collection. Therefore, during the intake process it is important to identify those persons.

2.Once these persons are identified, they must go through the informed consent process.

3.Information must be collected separately for each family member, rather than collecting data for the family as a whole.

Best Practices:

1.Agencies should collect data for HMIS on individuals or families who are not homeless and are receiving services from the agency. One of the greatest benefits of HMIS to an agency is the ability to create reports describing its' clients' characteristics, outcomes of the services they receive, and general agency operating information. Entering only HMIS data for homeless persons will give the agency only a partial picture. By including homeless and non-homeless persons in HMIS, agencies will be able to generate reports that wholly describe their operations.

2.Agencies should collect data for HMIS on individuals or families that make contact with the agency, but are not able to receive services from the agency. HMIS possesses the ability to count the persons that attempt to enroll in an agency's programs/services, even though they may not actually end up receiving those services. The agency will be able to create reports about the characteristics of these individuals, and use this information for a number of reasons. The agency could use this data to determine if they are being improperly referred to, or to quantify the additional need to funders.

6.2 Privacy Policy Notice

Policy: The Colorado HMIS Privacy Policy Notice must be appropriately posted within an agency.

Effective Date: *May 10th, 2005*

Description:

The Privacy Policy Notice is a brief document which describes a consumer's data rights in relation to HMIS.

Procedures:

1.Add the Agency Name into the Privacy Notice before printing and posting it.

2.Each workstation, desk, or area that is used during HMIS data collection must post the Colorado HMIS Privacy Policy Notice.

3.If an agency serves Spanish-speaking clients, the agency must also provide the translated Spanish version of the Colorado HMIS Privacy Policy Notice.

4.If an agency has a website, the Colorado HMIS Privacy Policy Notice must be posted on that website.

Best Practice:

An agency could also post the Colorado HMIS Privacy Policy Notice in a waiting room, an intake line, or another area where clients congregate before intake occurs. This will give clients another opportunity to read the notice before receiving services.

6.3 Informed Consent & HMIS Participation

Policy: Agencies must decide by program to obtain informed consent through one of these methods: inferred, verbal, or written.

Effective Date: *August 19th, 2005*

Description:

The Final HUD HMIS Data and Technical Standards allows agencies to collect data through implied consent given the circumstances of collection. Additional privacy protections for express consent such as verbal and/or written are optional.

Implied consent: HMIS data collection is explained and the client gives their information freely, without directly being asked to participate.

Verbal consent: The client verbally agrees/disagrees to participate in HMIS data collection.

Written consent: The client signs a form to agree/disagree to participate in HMIS data collection.

Agencies can decide by program how to obtain informed consent based on what is the most practical method for that program (e.g. verbal consent for call-based referrals vs. written consent for housing programs). That decision must be consistent for that program, meaning a program should not switch between consent methods.

Procedures:

1.Agencies must formally decide by program which consent method will be used to obtain the consent of clients.

2.The program must consistently use the same method for obtaining consent.

3.Agencies will follow the minimum guidelines for achieving implied consent, and subsequently can utilize the Best Practices Section for verbal and written consent.

Policy: When using informed consent for a program, the agency must obtain informed consent fairly, and in good faith when collecting HMIS data.

Effective Date: *October 7th, 2005*

Procedures:

1.Only an authorized HMIS user who has completed the HMIS Policies & Procedures training may obtain consent from clients.

2.An HMIS user must obtain consent from clients in respect, fairness, and in good faith for both the client and HMIS (meaning the explanation of HMIS, data collection, client rights, etc in an objective manner).

3.The HMIS user must adhere to the agency's decision for that program regarding the method of obtaining consent.

Policy: Unaccompanied youth who are at least 15 years old may give consent to collect information without parental/guardian consent. Parental/guardian consent can override the youth's consent. It is not possible to get consent of an unaccompanied youth under the age of 15 without parental consent.

Effective Date: *November 11th, 2005*

Procedures:

1.If an unaccompanied youth is obtaining services from the agency and they are at least 15 years old, you can get consent of the youth to participate in HMIS.

2.Any youth under the age of 15, you cannot get their individual consent. You must get parental/guardian consent to allow them to participate in HMIS.

3.Parental/guardian consent for a youth can override a youth's decision to participate. In the case where a youth has consented, and a parent/guardian does not consent, follow the revocation procedures.

Policy: Each program within an agency should strive to collect consent/information on adults that are present, and when necessary to operate their program, are allowed to collect consent/information on adults that are not present.

Effective Date: *October 7th, 2005*

Description:

Within agencies, it is sometimes required to collect information on adults that are not present in order to fulfill funder reporting requirements. The agencies must know who comprises the household and some of their basic information, including adults that may not be present. Emergency service programs often are the types of programs that must meet these standards. Agencies within longer term programs (like transitional housing, permanent supportive housing) are more likely to meet with all household members. Therefore, there is a greater possibility of obtaining consent and information from each adults directly.

Procedures:

1. Each program within an agency will need to determine if they will allow the collection of consent/information on non-present adults within the household.
2. When this situation presents itself, the agency and its users will continue to keep in mind the confidentiality and client rights of the non-present adult(s).
3. Whatever decisions the presenting adult makes regarding participation, will also apply to the absent adults in the household.

Best Practice:

When this situation presents itself, and it is necessary to collect information on an adult who is not present, give a copy of the Privacy Notice to the presenting adult to share with the other household members. This will inform the clients of their rights in case they wish to revoke their participation.

Policy: To obtain implied consent, agencies must have the privacy notice posted at each place that collects client data to satisfy this requirement.

Effective Date: *August 19th, 2005*

Best Practice:

Agencies could also use the following language with their clients before collecting their information:

"We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless and at-risk persons, and to better understand the needs of homeless and at-risk persons. We only collect information that we consider to be appropriate."

Policy: Agencies should strive to communicate informed consent in a language the client understands.

Effective Date: *August 19th, 2005*

Procedures:

If an individual or family does not speak English, the agency should attempt to obtain consent to the best of their abilities in a language the client understands. Written materials are currently available in English and Spanish.

Best Practice:

If your agency currently works with a translator and they can translate the Privacy Notice and Informed Consent documents, please share them with the HMIS System Administrators. They can post and share the materials to help the entire community.

Policy: Agencies cannot deny services to an individual solely on the basis of the individual deciding not to participate in HMIS.

Effective Date: *May 10th, 2005*

Procedure:

When an individual decides not to participate in HMIS, an agency cannot deny them services solely for that reason. However, agencies may need information from the client in order to provide services (for example, social security number needed to secure TANF benefits). In cases like this, agencies are not required to guarantee services.

Best Practice:

Agencies could determine if an individual will or will not receive services before the individual goes through the informed consent process. This will eliminate a perceived relationship between HMIS participation and service delivery.

Policy: Programs collecting written or verbal consent will offer at a minimum two options, and a maximum of four options regarding participation levels.

Effective Date: *May 25th, 2006*

Procedure:

1.A program conducting written or verbal consent must offer the client at least two options, one of which must be a 'Yes' to participate in the study and the other options must be a 'No' to participate in the study.

2.If clients choose the 'Yes', the agency may choose which of three methods of participation they will consistently use. These are the three methods:

- "Agree to let this Agency enter my information into Colorado HMIS": This means that their information is entered into the system, with personal identifying information shown (but secured through software and application security). They do have the right to refuse any specific question that is asked.
- "Use a special tool to hide my personal identifying information": Users will use the PIN Generation Tool in order to take in this client information, and generate a PIN. This will effectively hide name, social security number, date of birth, and gender.
- "Enter in my information, but then erase my personal identifying information": Users will use the Do Not Save feature within Tapestry in order to erase the name and social security number.

3.Programs that choose to use the PIN Tool as their primary 'Yes' method, must also record in the Year for Birth, and Gender for reporting purposes. There is no way to extract this

information from the PIN generated, and is critical to many agency and community reports.

4.Programs must offer a 'No' option which states "Do not include my information in the HMIS study": Individuals who choose this option are deemed as non-participants, and their information will not be included in any HMIS Community Reports. Agencies may still collect data necessary for their business operations and can optionally record it in the database.

5.Programs can offer more than one 'Yes' option, allowing for up to all three 'Yes' options to be presented to the client.

Best Practices: Expressed Consent

For those agencies that decide that their program will collect expressed consent (verbal or written), the following best practices have been assembled. These best practices focus on situations that are applicable to either type of consent.

Presumption of Competency: Clients are presumed to be competent, unless there is a known court order claiming their incompetence.

Effective Date: *August 19th, 2005*

Recommendations:

1.An industry-wide best practice is to presume that all clients are capable of competency, unless there is a known court ordering stating otherwise.

2.If there is a known court order stating the individual is not competent enough to make informed decisions, then it will not be possible to obtain informed consent for HMIS. In this case, the HMIS user should treat this user as a non-participant.

3.HMIS users should do their best in attempting to obtain informed consent from individuals that may appear to be not fully competent during intake, in which there is no court order. If it is not possible to obtain a truly informed decision regarding HMIS participation, the individual should be dealt with as a non-participant in HMIS.

4.Often individuals may be temporarily incompetent because they are under the influence of a particular substance, which affects their ability to make a decision. If it is possible, delay the informed consent and HMIS data collection, under they are no longer under the influence and are able to make decisions.

Physical Copy: Agencies may give the clients a copy of the privacy notice/informed consent agreement, which notifies the client of their rights.

Effective Date: *August 19th, 2005*

Recommendations:

1.After a client consents to participating in HMIS/data collection, the agency may give the client a physical copy of the privacy notice, informed consent agreement, or other document which notifies the client of their information rights.

2.For agencies that have programs that are collecting written consent, they may also wish to provide clients with a photocopy of the signature page so that they have a record of their HMIS participation decision.

Participation Options: The agency should verbally explain the choices available to the client for HMIS participation.

Effective Date: *May 25th, 2006*

Recommendations:

Below are the possible explanations for each one of 4 possible choices that could be offered to a client:

1. "Agree to let this Agency enter my information into Colorado HMIS": This means that their information is entered into the system, with personal identifying information shown (but secured through software and application security). They do have the right to refuse any specific question that is asked.
2. "Use a special tool to hide my personal identifying information": Users will use the PIN Generation Tool in order to take in this client information, and generate a PIN. This will effectively hide name, social security number, date of birth, and gender.
3. "Enter in my information, but then erase my personal identifying information": Users will use the Do Not Save feature within Tapestry in order to erase the name and social security number.
4. "Do not enter my information": Individuals who choose this option are deemed as non-participants, and their information will not be included in any HMIS Community Reports. Agencies may still collect data necessary for their business operations and can optionally record it in the database.

Non-Participants: Agencies can optionally record individuals within the HMIS software who choose not to participate, as long as they accurately mark this in the system so HMIS System Administrators do not include that information in community reports.

Effective Date: *November 11, 2005*

Recommendations:

1.A number of individuals will either choose not to participate in HMIS or are not capable of informed consent (for a variety of reasons), however, it is important for reporting purposes that

these individuals are still counted.

2.Agencies can enter these records in the software, as long as the record shows that they are NOT INTERESTED in participating in the HMIS study. This will allow agencies to fully utilize the Tapestry software as their internal client database without having to keep track of non-participants separately.

3.Subsequently, HMIS System Administrators agree to not include information from non-participating individuals in any community reports.

Best Practices: Verbal Consent

For those agencies that decide that their program will collect verbal consent, the following best practices have been assembled.

Script: Agencies should develop a standard script in order to collect client's verbal consent.

Effective Date: *August 19th, 2005*

Recommendation:

"We would like to ask your permission to collect information about you. By law, we must protect your privacy, tell you about your rights, and tell you how we keep your information private. We may use and disclose your information in the following ways: providing or coordinating services for you, operating our programs, reporting without identifying your specific information to organizations who give us money to run our programs as well as for research purposes, and when required by law – such as a life-threatening situation to you or others, and/or suspicion of child abuse or neglect. Any other use of your information is not allowed without your approval. Your information will be kept seven years after you stop getting services. You have the right to access the data you provide, and can change it if it isn't correct. If you ever feel that your privacy rights were violated, you have the right to file a complaint. You have the right to cancel your consent at any time, however, information that has already been collected remains in the system and personally identifying data is hidden. You have the right to receive services when available, even if you choose not to participate in HMIS. There are a number of technical and procedural security protections in place to keep information about you safe. Additionally, only authorized staff from this agency and administrators of the system have access to your data. You have the following choices:

- Agree to let us enter your information
- Agree to let us enter your information using a special tool to hide your personal identifying information
- Agree to let us enter your information, and then erase your personal identifying information
- Not participate at all

Which of those options would you like to choose?"

Best Practices: Written Consent

For those agencies that decide that their program will collect written consent, the following best practices have been assembled.

Verbal Explanation: Even if your agency is collecting written consent, you should verbally explain the informed consent form before the client signs it.

Effective Date: *August 19th, 2005*

Recommendations:

1.Agencies can still use a verbal script, like the one provided in the best practices, to explain the nature of collecting client data and their rights.

2.Verbally explaining the written consent before the client receives the form will help ensure participation.

3.Clients will have the opportunity to ask questions at this time to clarify anything that they may not have understood based on the form.

Consent Form Review: Agencies should review the consent form with the client to ensure that it was filled out appropriately, and then sign as a witness.

Effective Date: *August 19th, 2005*

Recommendation:

1.Serving as a witness to the signing of an informed consent form is a good way to ensure quality control for informed consent (that it was filled out in-line with agency policies).

2.Witnessing the signing, also allows agencies to go back to the individual(s) involved if any questions arose about the form.

Storing Informed Consent: Informed consent forms should be stored securely from a minimum of seven years after the client last received services from the agency.

Effective Date: *August 19th, 2005*

Recommendations:

1.The informed consent form is valid for seven years after the client last received services from the agency for the purpose of determining valid participation choices. Therefore, for auditing purposes it is important to keep the informed consent form collected for at least that length of time.

2.Informed consent forms must be kept securely in accordance with standard confidentiality and privacy practices (e.g. Locked away in a file cabinet, and not accessible without authorization).

3.It is recommended that agencies keep the informed consent form in their current client file with the other information being collected and maintained. It will be easier to locate their information in this manner, rather than creating a separate file just for HMIS, unless client files are purged prior to seven years after the client last receives services.

4.If an agency does not currently keep client files, it will be important to set up a file system to keep track of the forms.

6.4 Using Paper-Based Data Collection Forms

Policy: Agencies may choose to initially collect client data on paper and enter it into the HMIS software later, rather than entering it directly in the system.

Effective Date: *May 10th, 2005*

Description:

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. HMIS paper-based forms that enable to collection of the Universal, Community, and Program-Specific standards are available.

Agencies that are required to collect only the Universal & Community data elements could use just the Universal Data Collection form.

For Agencies that are required to collect all of the data elements, there are four forms that agencies could use:

- Head of Household Intake form
- Other Household Member Intake form
- Service Delivery Tracking form
- Discharge form

During the HMIS Policies & Procedures training, HMIS Users will learn how to use these forms to fulfill their data collection obligations.

Procedures:

1.Agencies may utilize the HMIS paper-based forms for initial data collection.

2.HMIS Users will have 5 business days from the point of the event (intake, service delivery, or discharge) to record the information into the HMIS software.

3.Universal and Program-Specific forms will be available to agencies. Agencies receiving funds from federal homeless assistance grants are required to utilize the Program-Specific forms. Agencies not receiving these types of funds may choose either one of the forms to use.

Best Practices:

1.Agencies that are not required to complete the Program-Specific data fields are strongly recommended to collect these pieces of information, depending upon the type of programs and services the agency offers. 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.

2.Agencies that wish to customize the forms to include their own required fields should contact the Colorado HMIS helpdesk to coordinate that effort, and ensure they meet the minimum standards.

6.5 Collecting Client Disability Information

Policy: Agencies must collect client disability information after the individual is enrolled into a program, unless it is a requirement for program entry.

Effective Date: *May 10th, 2005*

Description:

As a part of the data standards required by HUD, agencies are requested to ask clients questions about disabilities. To comply with other federal laws and regulations, these client questions must be asked at a certain point in time to avoid any legal issues.

HUD defines 'disabling condition' as: "(1) a disability as defined in Section 223 of the Social Security Act; (2) a physical, mental, or emotional impairment which is (a) expected to be of long-continued and indefinite duration, (b) substantially impedes and individual's ability to live independently, and (c) of such a nature that such ability could be improved by more suitable housing conditions; (3) a developmental disability as defined in section 102 of the Developmental Disabilities Assistance and Bill of Rights Act; (4) the disease of acquired immunodeficiency syndrome or any conditions arising from the etiological agency for acquired immunodeficiency syndrome; or (5) a diagnosable substance abuse disorder.

Procedures:

1.If the agency's program requires the individual to be disabled, then the agency may ask the client the disability questions before program entry or after program entry (e.g. like a Shelter Plus Care program).

2.If the agency's program does not require the individual to be disabled, then the agency must ask the client the disability questions after program entry.

6.6 HMIS Data Standards

Policy: All agencies and HMIS users are required to collect HUD's Universal Data Standards fields and community reporting fields, as stated in the Agency Agreement and End User Agreement.

Effective Date: *May 10th, 2005*

Description:

HUD requires all agencies participating in HMIS to collect a standard set of client information, known as the Universal Data Standards. Examples of the Universal Data fields includes: name, social security number, birth date, ethnicity, and race. Within our community, there are additional fields that are also required in order to produce the necessary aggregate reports. Such fields include: are you homeless, how many times have you been homeless in the last 3 years. This allows the CoC to determine the extent of chronic homelessness.

Procedures:

1.Agencies and HMIS Users will collect all of the Universal Data fields for its clients that choose to participate in HMIS.

2.Agencies and HMIS Users will collect all of the community required fields for its clients that choose to participate in HMIS.

Best Practices:

Agencies may decide to also add more fields to its required data collection, that are incorporated into its own HMIS policies. This is particularly beneficial when HMIS is capable of collecting all of an agency's information needs, but the fields are not incorporated into the Universal or community data standards.

Policy: HMIS users are required to collect HUD's Program-Specific Data Standards fields, if the client is receiving services funded through federal homeless assistance grants, as stated in the Agency Agreement and End User Agreement.

Effective Date: *May 10th, 2005*

Description:

HUD requires agencies who receive federal homeless assistance grants to complete the Program-Specific Data Standards. Examples of the Program-Specific fields includes: income, education, employment, military service details, and health information.

Procedure:

1.Agencies and HMIS Users will collect all of the Program-Specific fields for its clients that choose to participate in HMIS, if the clients are receiving services through federally-funded homeless assistance grants.

Best Practices:

Agencies that are not required to complete the Program-Specific data fields are strongly recommended to collect these pieces of information, depending upon the type of programs and services the agency offers. The additional data points on the client will prove extremely helpful for the agency when reporting on client outcome measurement/progress, internal accounting for services delivered, and external reporting to funders.

Policy: HMIS users are required to ensure data quality of the information that they collect for HMIS, as stated in the End User Agreement.

Effective Date: *May 10th, 2005*

Description:

There are a number of reasons why data quality is important to everyone, from client to user to agency to community perspectives. If information is not collected accurately, clients may experience issues trying to coordinate multiple services, receiving appropriate referrals, and eligibility determination for services. HMIS Users may experience issues serving these clients without accurate information being collected and maintained. Agencies and the community will have reporting issues. Reports generated from HMIS are only as good as the information entered into HMIS. Without high quality data going into HMIS, the information contained within the reports will not be as solid.

Procedures:

1.HMIS Users will collect data and ensure the quality of the information by reviewing the information that the client gives for HMIS.

2.HMIS Users will attempt to correct any identified data quality issues that are shown during the Data Quality Audit performed by HMIS System Administrators.

Best Practices:

HMIS Users should review all data the client gives for HMIS purpose to ensure its quality and consistency, as the information is being turned in or collected. If possible, HMIS Users could walk through the data collection process with the client catching potential issues along the way.

6.7 Sharing Client Data

Policy: HMIS client data may not be shared unless explicitly authorized by the client.

Effective Date: *May 10th, 2005*

Description:

Agencies tend to work with a number of other service providing agencies while coordinating services for a client. While coordinating services, it is important to keep the client's identity confidential, unless the client expressly permits their information to be shared.

Procedures:

1.HMIS Users will keep client data confidential at all times, and will obtain client permission to disclose personally identifying information only when necessary.

2.In the future, electronic data sharing between agencies will be enabled with agency and client consent regarding what agencies have access to their information, and what information they would like to share.

6.8 Client Access to Their Information

Policy: Clients have the right to a copy of their Universal, community, and Program-Specific data contained within Colorado HMIS.

Effective Date: *May 10th, 2005*

Procedures:

1.Clients will request a copy of their information contained within Colorado HMIS.

2.Agencies are required to provide them a print out from Colorado HMIS of the Universal, community, and Program-Specific data elements.

3.Agencies are not required to print out any additional information, although it is optional and allowed.

Best Practices:

1.Case management notes are typically not shared with the client. However, consider providing the client related information such as their Goals, Outcomes, Referrals, & Services Provided.

2.If utilizing paper forms with data entry into Colorado HMIS occurring later, consider making a photocopy of the paper forms for the client if they request a copy.

3.If entering data directly into Colorado HMIS without utilizing paper forms, consider automatically printing a copy of the information for the client.

6.9 Filing A Grievance

Policy: Clients have the right to file a grievance regarding potential violations of their privacy rights regarding HMIS participation.

Effective Date: *May 10th, 2005*

Procedures:

1.A client must request and complete the grievance form from the agency.

2.The client may decide to turn the form into an agency manager or another person of authority not related to the grievance OR may mail the form to the Colorado HMIS team directly.

3.If the agency receives a completed grievance form, they must submit it to the Colorado HMIS team promptly.

4.The Colorado HMIS team will review the grievance, research the nature of the complaint, and will respond within 30 days.

Policy: No action or punishment will be taken against a client if they choose to file a grievance.

Effective Date: *May 10th, 2005*

Procedure:

1.The agency named in the grievance, the Colorado HMIS team, and other participating HMIS agencies will not refuse or reduce services to the client because of filing a grievance.

2.A thorough investigation will occur if a client reports retaliation due to filing a grievance.

6.10 Revoking Authorization for HMIS Data Collection

Policy: Clients who initially agree to participate in Colorado HMIS have the right to rescind their permission for data collection.

Effective Date: *May 25th, 2006*

Procedures:

1.Clients must request and complete the Revocation Form from the agency.

2.The agency will file the Revocation Form. Ideally this would reside with the client's previously signed Informed Consent Agreement if collecting written consent.

3.In Tapestry, the user must edit the client's record and set the Status to 'WITHDRAWN'.

4.When practical for the agency (not using Tapestry as their internal client system), the user may also check the 'DO NOT SAVE' option too.

7. HMIS Software Processes

7.1 Reduce Duplicates in HMIS for your Agency

Policy: In order to reduce the duplication of client records, HMIS Users should always search for the client in HMIS before creating a new client record.

Effective Date: *May 10th, 2005*

Description:

It is often very easy to create multiple records in the system for the same individual being served at the same agency. When client records are duplicated, it is very difficult for other HMIS users to work with that individual's records as they attempt to put in case management notes, goal planning, and other information. Without performing this simple task, agencies' reports will be corrupted with inaccurate information.

Procedures:

1.When an HMIS User is collecting data from an individual or family, the HMIS User will run a search within HMIS to determine if this individual already exists in the system.

2.It may be possible that this person already exists, but chose to have just their PIN recorded instead of their name, social security number, and birth date. It may be required to look in the paper files to determine their PIN.

3.If this person does not exist, then the HMIS User should create a new client record.

Best Practices:

1.Perform a couple of types of searches when attempting to find an existing record. Clients often don't use the exact same name that was previously entered.

2.Try to use a field other than name that tends to be more accurate, and not open for much interpretation (birth date, social security number, etc.).

7.2 Entering Data based on Informed Consent Decision

Policy: HMIS Users must enter data into HMIS in a manner consistent with the client's decision on how they chose to participate.

Effective Date: *May 10th, 2005*

Description:

When the client chose to participate in HMIS, they made a selection on the Informed Consent form stating how they would like to participate (all, PIN Generation Tool, Do Not Save). When the HMIS User is entering their information into the system, they must abide by that decision.

Procedures:

1.If a client chose 'Agree to let this Agency enter my information into HMIS' then the HMIS User should just enter all of their information provided, like normal data entry.

2.If a client chose 'Agree to let this Agency enter my information using the PIN Generation Tool':

- After clicking on new client record, on the General Information tab the HMIS User should click on the HMIS PIN Generation Tool link.
- The HMIS User should enter the information requested within the PIN Generation Tool. After completing data entry, the HMIS User should click the Generate PIN button.
- The PIN for this individual will be created. The HMIS User must write down their PIN on the Intake and Informed Consent form.
- The HMIS User can then close the HMIS PIN Generation Tool window.
- Back in the General Information tab, the HMIS User should enter the PIN number into the PIN field (just below the HMIS PIN Generation Tool link).
- The HMIS User can continue entering in the client's non-personally identifying information.

3.If a client chose 'Agree to let this Agency enter my information using the Do Not Save feature':

- After clicking on new client record, the HMIS User should enter all of the client's information in the General Information tab as normal.
- The HMIS User should then click the checkbox next to 'Do Not Save' located to the left of the client's PIN.
- When the HMIS User clicks Save on this tab, the client's personally identifying information will be cleared but the PIN will remain instead.

7.3 Client Intake - Completing Required Fields in HMIS

Policy: During client intake, HMIS Users must complete the Universal and Community required fields for all clients, and the Program-Specific fields if required.

Effective Date: *May 10th, 2005*

Description:

All agencies are required to complete the Universal and Community fields, regardless of funding sources. Agencies that receive homeless assistance grant funds are required to complete the Program-Specific fields. Agencies not required to complete the Program-Specific fields, may choose to implement this standard for their agency anyway. HMIS Users are required to abide by the data collection rules already set forth.

Procedures:

1.To complete the Universal and Community required fields for intake, HMIS Users must go to the General Information, Homeless Management, & Intake tabs and respond to the fields marked required.

2.To complete the Program-Specific required fields, HMIS Users must also go to the Domestic Abuse, Income & Benefits, Education, Employment, Military & Veterans, & Health tabs and respond to the fields marked required.

Best Practice:

HMIS Users should be aware of their agency's data requirements and internal standards. Agencies may decide to collect additional pieces of information outside of the Universal, Community, and Program-Specific fields that are needed for its own operations and funding sources. This guide merely establishes the minimum or baseline level of required data.

7.4 Service Delivery Tracking Requirements

Policy: HMIS Users within agencies that are required to complete the Program-Specific fields, must record each service delivered to the client.

Effective Date: *May 10th, 2005*

Description:

All agencies have the ability in HMIS to track what services they have provided to clients, however some agencies are required to collect this information. This information is used for reporting purposes (APR, AHAR, etc.) This information can be used in very creative ways to help agencies with operations, decision-making, and reports to funders.

Procedures:

1.When required by either HUD or Agency standards, HMIS Users will record into HMIS the dates, and services provided to each client in the system.

2.HMIS Users will utilize the Intake tab to complete the required fields.

7.5 Client Discharge – Completing Required Fields for HMIS

Policy: During discharge or program exit, HMIS Users must complete the Universal and Community required fields for all clients, and the Program-Specific fields if required.

Effective Date: *May 10th, 2005*

Description:

During client discharge from a program, there are additional data collection requirements. Again, all agencies must complete the Universal & Community fields. Agencies that are required to also collect Program-Specific information have additional data to collect.

Procedures:

1.To complete the Universal and Community required fields for discharge, HMIS Users must go to the Intake tab and enter the Program Exit date.

2.To complete the Program-Specific required fields, HMIS Users must also go to the Homeless Management, Income & Benefits, Education, Employment, & Health tabs and respond to the fields marked required.

7.6 Revoking Authorization for HMIS Data Collection

Policy: Clients who initially agree to participate in Colorado HMIS have the right to rescind their permission for data collection.

Effective Date: *May 10th, 2005*

Procedures:

1.Clients must request and complete the Revocation Form from the agency.

2.The agency will file the Revocation Form with the client's previously signed Informed Consent Agreement.

3.The agency will no longer collect and enter data for HMIS purposes.

4.The agency will access the client's record in HMIS and perform the following:

- In the General Information tab, click the 'Do Not Save' box.
- Click the Update button at the bottom of the tab.

7.7 Electronic Sharing of Client Records

Policy: Although not currently implemented, HMIS will enable agencies to share client records electronically if both agencies agree AND the client consents to the sharing of their information.

Effective Date: *May 10th, 2005*

Description:

Eventually HMIS will allow groups of agencies to share the same client record, as they try to provide coordinated services for the individual/family. This feature is not currently available, although planning is occurring right now. Agencies who wish to have the ability to share records with one another will need to sign an agreement between each other. Clients will also have the added ability to decide if they want their information shared with another agency, as well as what information they would like shared. The Colorado HMIS Helpdesk will notify agencies when this feature is available in the software, and the required forms and agreements are available too.

8. HMIS Quality Assurance

8.1 Data Quality and Correction

Policy: Site Administrators are required to fix data quality issues within 5 business days of receiving the month data quality report.

Effective Date: *May 10th, 2005*

Description:

To produce high quality, reliable reports it is imperative to possess high quality data. HMIS System Administrators 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.

Procedures:

1.At the end of each month, HMIS System Administrators will review the quality of each agency's data by running reports out of HMIS.

2.HMIS System Administrators will then distribute to each agency's Executive Director and Site Administrator a scorecard of the results based on their agency's data.

3.Site Administrators are required to work with the HMIS System Administrators to rectify any shortfalls on data quality, and fix issues within 5 business days.

8.2 Security Auditing

Policy: Site Administrators are required to immediately resolve any issues discovered during an HMIS security audit.

Effective Date: *May 10th, 2005*

Description:

In order to maintain the high level of security, client privacy and confidentiality practices set up in this policies and procedures document, security audits will be conducted by HMIS System Administrators on a regular basis. Site Administrators will work with the HMIS System Administrators to schedule an audit, and to assist HMIS System Administrators in performing the audit. The audit will cover many topics, and includes: informed consent agreement, privacy notices, technology security, and data entry practices. The details of the audit can also be found in the HMIS Quality Plan.

Procedures:

1.HMIS System Administrators will notify the agency's Executive Director and Site Administrator of an upcoming audit. The audit will be scheduled ahead of time, as there will be no surprise audits.

2.HMIS System Administrators will perform the audit and create a results report. This report will be submitted to the agency's Executive Director and Site Administrator.

3.Any deficiencies in practices or security must be resolved immediately. If necessary, a follow-up audit will be conducted to ensure that the changes have taken affect.

8.3 Additional Quality Reports

Policy: HMIS System Administrators will make additional quality reports available regarding software, helpdesk, training, and overall program directions.

Effective Date: *May 10th, 2005*

Description:

As outlined in the HMIS Quality Plan document, there are additional reports that will be created to ensure that the overall HMIS program is of high quality. Topics that will be reported on will include overall software quality, quality of the helpdesk, training quality, and overall program quality. As these reports are available, HMIS System Administrators will notify agencies.

9. Colorado HMIS Helpdesk Procedures

9.1 Contact Your Site Administrator First

Policy: HMIS Users should attempt to contact their agency's Site Administrator first before contacting the HMIS Helpdesk.

Effective Date: *May 10th, 2005*

Description:

Agency Site Administrators will be the best resource for finding out specific information regarding its agency's policies and procedures as they relate to HMIS. They are also going to be the most knowledgeable and accessible person regarding software and its capabilities.

Procedures:

1.HMIS Users should first try to contact their agency's Site Administrator to resolve their issue.

2.If the Site Administrator is unavailable or is not able to resolve the issue, HMIS Users should feel free to contact the Helpdesk.

9.2 Ways to Contact the Helpdesk

Policy: HMIS Users should attempt to use the online request form to contact the HMIS Helpdesk with their issues.

Effective Date: *May 10th, 2005*

Procedures:

1.Registered HMIS Users can fill out the online request form at (available soon): http://www.cdhs.state.co.us/shhp/homeless_programs/hmis/issues.html

2.HMIS Users can also email the Helpdesk: colorado.hmis@state.co.us

3.HMIS Users can also call the Helpdesk (303) 866-7109

4.HMIS Users can also fax the Helpdesk (303) 789-6950

9.3 Response Times for Issues

Policy: The HMIS Helpdesk will attempt to resolve issues within the shortest period of time possible, but are subject to software response times to VisionLink for some issues.

Effective Date: *May 10th, 2005*

Description:

The HMIS Helpdesk is generally available between the hours of 8 a.m. To 5 p.m. Monday through Friday. While the helpdesk can answer most questions and concerns regarding HMIS, when there is a direct issue with the system the helpdesk is subject to VisionLink's response times.

Procedures:

1.After receiving an issue, the HMIS Helpdesk will respond to issues in the order they were received. If the issue cannot be resolve by the HMIS Helpdesk, and VisionLink is required, the HMIS Helpdesk will notify the HMIS User accordingly.

2.During normal business hours, HMIS System Administrators & VisionLink's response times are typically as follows:

Severity	***Description***	***Response Time***
1 Critical	Major system or component is inoperative which is critical to the Partner Agency's business.	Contact VisionLink within 1 hour and notify Partner agency of action plan and resolution within 2 hours.
2 High	Partner Agency is impacted by service delay but is still able to maintain business function.	During SA normal business hours, SA will initiate problem resolution within 4 hours and notify Partner Agency of action plan and resolution within 6 business hours.
3 Medium	The problem has a reasonable circumvention and the Partner Agency can continue with little loss of efficiency.	During SA normal business hours, SA will initiate problem resolution within 8 hours and notify Partner Agency of action plan and resolution within 12 business hours.
4 Low	The call requires minor action or is for informational purposes only.	Response time within 24 business hours.

10. HMIS Software Security Procedures

10.1 HMIS Software System-Level Security

The HMIS software is secured physically through a number of best practices, and results in high-level security at the most basic level. Several of these system level security features include:

- Separation of the database and application on different servers
- Multiple layers of firewalls between database, application, and users
- Encryption of the data on the database
- Undisclosed location of the physical servers
- Physical servers are locked down, in secured fire-safe rooms

10.2 HMIS Software Application-Level Security

Within the HMIS software itself, there are additional layers of security built into the system. This results in making the system harder to access without appropriate permissions. These security features include:

- 128-bit encryption of the connection between a HMIS User's computer and the HMIS application
- Users are organized into security groups, in which the groups are given specific permissions on what they can access in HMIS
- Passwords are automatically and randomly generated, thereby enforcing strong password protection. This means that it would not be possible to guess one's password based on social knowledge of the person (e.g. Dog's name, maiden name, favorite activities, etc.)
- An HMIS User's connection to the application will automatically close down after a period of time of inactivity in the HMIS software.
- There are logging and audit systems in the background recording each user's activities in adding, viewing, and editing information.
- HMIS Users are only authorized to see its own agency's data

10.3 Workstation Security Procedures

Statistically, most security breaches are due to human error rather than systematic issues. In order to keep the application and data secure, HMIS Users must also implement some additional security measures.

Policy: HMIS User's computer screens should be placed in a manner where it is difficult for others in the room to see the contents of the screen.

Effective Date: *May 10th, 2005*

Description:

The placement of one's monitor can play a small role in establishing security at the agency. HMIS Users should consider placing the monitor in a way that it is difficult for others to see the screen without you knowing it. Good placement: When someone walks into the room with the computer, all they can see is the back of it. Bad placement: When someone walks into the room, they can look over your shoulder without you knowing it, and read material off the screen.

Policy: Do not write down your username and password, and store it in an unsecured manner.

Effective Date: *May 10th, 2005*

Description:

With the username and password into HMIS being complex, it will not be easy to remember it in the beginning. Most people will write down or print out the login information. When one does this, make sure to keep this information in a locked drawer or cabinet. Do not post this information under your keyboard, on your monitor, laying out for others to see. This type of behavior can lead to large security breaches.

Policy: Don't ever share your login information with anybody (including Site or System Administrators).

Effective Date: *May 10th, 2005*

Description:
If someone is having trouble accessing HMIS, contact your Site Administrator or the HMIS System Administrators. When persons are caught up in performing tasks on the computer, and one person is locked out of the system OR needs information from the computer, it is easy to simply share your username and password with them. First, this is a severe violation of the User Agreement. Secondly, while this person may be someone trusted within the agency they may do something accidentally or even intentionally under your login. With the auditing and logging mechanisms within HMIS, any changes this other person makes or actions that they do will be tracked back to your login. When we review the data and security logs, we will look back to you as being responsible for whatever might have occurred. There is no sense taking the blame for something someone else did; and this whole situation can be avoided by simply not sharing your login information.

Policy: When you are away from your computer, log out of HMIS or lock down your workstation.

Effective Date: *May 10th, 2005*

Description:

Stepping away from your computer while you are logged into HMIS can also lead to a serious security breach. Although there are timeouts in place to catch inactivity built into the software, it does not take affect immediately. Therefore, anytime when you leave the room and are no longer in control of the computer, you must do one of two things. First, you can lock down your workstation. Most Windows-based operating systems allow users to lock their workstation by simply pressing CTRL-ALT-DELETE keys, and choosing "Lock Workstation". This will require users to simply enter in their Windows password when returning. Secondly, if this is not an option for you, then at a minimum log out of HMIS.

11. HMIS Data & Reporting

11.1 Exporting Data

Policy: Data Export ability will be made available only to MDHI HMIS System Administrators and Agency Site Administrators.

Effective Date: *June 22, 2006*

Description:

The purpose of limiting ability to export client level data to the System Administrators and Site Administrator is to control the structure, utilization, and location of the information. The primary goal is to protect the personal identifiable information.

Policy: Comply with CO House Bill 06-1119 concerns a breach of data security

Effective Date: *June 22, 2006*

Description:

CO House Bill 06-1119 describes the steps required by law to take when a breach of data security occurs. If data is in an unsecured format and the info that gets stolen includes: name and either SSN / Drivers License / financial account number then you must do the following: contact those person(s) if possible, notify major statewide media, post notice on your website, contact all consumer reporting agencies. Contact SHHP if a situation arises.

Policy: Never export SSN for clients.

Effective Date: *June 22, 2006*

Description:

Agency is responsible for the protection of client information. The Site Administrator is the first line of defense when exporting information and will uncheck SSN before performing the export of the General Information Tab and Household Tab. The Site Administrator is also responsible for the appropriate storage and clean-up of the files created when doing an export, expansion, or conversion of data. Any management or operational reports generated from exported data also requires additional protection. MDHI HMIS user group recommends these best practices:

- Limit access within your organization to files (any form) with Personal Identifiable Information (name, birth date from General Information Tab export). When ever-possible strip name and birth dates (convert birth date into age). Provide the information only to people that "need to know" in the organization. Operational and management reports contain minimal personal identifiable information.
- Keep any form of the electronic files secure (zip, expanded, converted) on a network drive with limited access, password protect files (don't backup)
- Delete the zip, expanded, or converted files after use – don't store file indefinitely.
- Properly dispose of paper copies of reports generated by shredding.

Policy: Do not store or save the zip, expanded or converted files containing exported information (i.e. excel, access format) on these portable media types: floppy disk, jump drive, cd, dvd

Effective Date: *June 22, 2006*

Description:

To protect the personal identifiable information exported from Colorado HMIS storage is limited to electronically secure location. Do not store Colorado HMIS information on portable media (i.e. floppy disks, jump drives, cds and dvds).