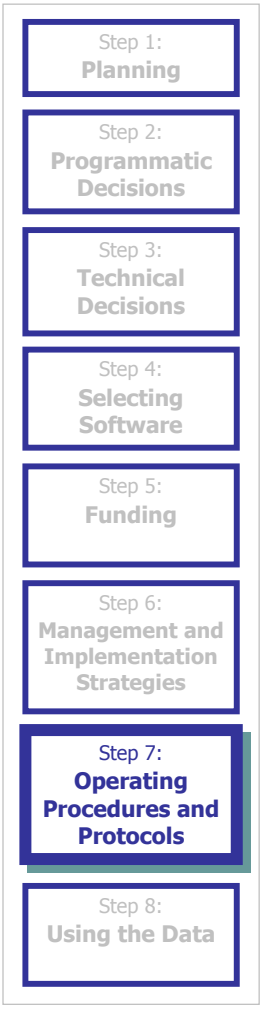
Step Seven: Implementing the System—Operating Procedures and Protocols



From system implementation, communities proceed directly into the overall project goal—operating a functioning HMIS. This step focuses on several tasks that need to be finalized prior to system operation, including development of SOPs, ensuring data accuracy, and stakeholder training. Some of the tasks described in this step need to occur in conjunction with the implementation tasks described in Step Six. All of these tasks build off of a community's vision, principles, and policies.

A host of operational issues are not discussed in this document because the guide focuses on the implementation process rather than long-term operations. In addition, to these preliminary operations steps, a community also needs to consider system maintenance (all of the activities to sustain the operation of the system) and system modification (ongoing system enhancement activities to improve and expand the system to keep pace with local needs). The HMIS management structure needs to include staff members or consultants with technical expertise to maintain the day-to-day system operations, user support, troubleshooting, and routine maintenance (See Step Six for management models).

Step Seven output:

- Standard Operating Procedures (SOPs) Manual.
- HMIS Training Curriculum.

Who Will Develop Operating Procedures and Protocols?

Step Six includes a substantive discussion on system management models, roles, and responsibilities. The management structure determined at the beginning of the implementation process should also assume ongoing operational responsibilities. Regardless of these management decisions, it is critical to continue to involve HMIS stakeholders in its operation, and in general leadership, advisory, and enforcement capacities. The same stakeholder groups should be represented although the specific individuals need not remain the same. Particular efforts should be made to engage consumer representatives for the governing board and project staff as their perspectives on policies, day-to-day management, training, and consumer participation are important to continued successful operation.

During the implementation and early operation phases, the planning group established in Step One should evolve into a formal governing board. As the vision and principles are codified into formal policies and procedures, the stakeholder group will act as the primary policymaking body and the system manager will implement these policies and procedures.

- HMIS steering committee (with representation from lead partners, including consumers and agency staff): Responsibilities include developing, monitoring, enforcing, and revising HMIS policies. The committee should design a penalty structure outlining sanctions for partners that fail to comply with written policies, such as limiting or terminating the partner's rights to access the

system. The entity should also consider an appeals process and structure. Committee responsibilities and sanction policies should be laid out in the SOPs.

- HMIS system manager (under the oversight of the stakeholder group): Responsibilities should include development of a formal SOPs manual with associated forms and contract documents to actualize steering committee policies; execution and maintenance of necessary agreements with participating agencies and staff members; development and implementation of initial and ongoing training of staff and participating agencies; and ensuring data integrity, analysis, and reporting of data (see Step Eight for use of data).

- Consumer representatives: Beyond participation on the HMIS steering committee, consumers can be hired as peer trainers to build their understanding of HMIS issues and client rights and alleviate their concerns; and as agency trainers to help agencies understand client confidentiality and improve client sensitivity and effective use of HMIS. Consumers can act as peer advocates to represent clients in disputes and lead consumer advisory groups. They can also be hired as consumer staff representatives to help the system management organization understand consumer issues, integrate them at all levels of system operation, review and monitor operational and project deliverables, and analyze the impact of HMIS on continuum and homeless services users.

Standard Operating Procedures

As discussed previously, communities need to agree on a standard set of guiding principles, policies, and procedures for operating the HMIS. The community should develop an SOPs manual to document specific expectations regarding the use of the system and indicate procedures that should be followed regarding routine and occasional functions. The manual should be developed prior to beginning implementation (it is important to budget time for this activity) and be regularly updated and distributed. Standardized forms used by participating agencies should be included in the manual. Different SOPs may be developed for the various types of users. For instance, one SOPs may ensure consistent procedures are followed by the system administration staff (central organization) while another may focus on end-users (agency staff). A training program should be developed to regularly train and update employees on policies and procedures.

This step provides a brief discussion of several important elements that should be included in an SOPs manual, including a discussion of privacy protection elements and data accuracy issues. See supporting materials for reference to a detailed outline of a sample SOPs manual.

Privacy protection protocols

Agencies may already be familiar with client privacy protocols related to case management and case files. These procedures must be supplemented with HMIS provisions of the policy that include parameters for inputting, revising, aggregating, and sharing client information with others. Protocols should ensure the safety of the most sensitive HMIS information and consumers, including victims of domestic violence.

- Informed consent

  Informed consent is the first component of a sound privacy protection policy. To generate communitywide data about homelessness, some level of data from the HMIS must be aggregated at the regional level. In some cases, dramatic improvements in service delivery can occur through interagency case management. None of these changes should occur at risk of exposing clients' private information without proper consent.

For clients to consent, they must be informed about the system. An appropriate oral explanation should include a description of the HMIS, its purpose, the security mechanisms and privacy measures in place, and benefits for clients. It is also appropriate to provide a written description that echoes the oral explanation for the consumer to keep for review. Consumers can serve as valuable resources in the development of effective oral and written descriptions. A trained peer advocate can help to clarify the distinction between oral and written consent, especially for those with domestic violence, justice system, or particular health concerns. Ideally this distinction would be explained to everyone whose information is entered into the HMIS. Individuals should understand exactly what they are consenting to, including the specific content of the information that will be shared.

After the HMIS has been explained, the intake or case management staff person should request client consent to enter the client information into the HMIS. Most HMIS have a box on the intake form (hard copy and/or digital) that denotes whether oral consent has been received from the client (see appendix G for a sample consumer system description).

Note that some funders (particularly Federal and other government sources) may require for reporting purposes that minimum data elements be collected in tandem with receipt of a publicly funded service. In these cases, consent may be limited to collection of data beyond those minimum elements and questions of how the data are used beyond reporting anonymously to funders. Regardless, individuals should be educated about the system and apprised of their rights.

- Written consent

Oral consent to participate in the HMIS does not indicate consent for identifiable client information to be shared among agencies. A community's SOPs should include an information release provision indicating that an agency will not release client identifiable information to other organizations without proper written client consent. The written consent procedure should document the information being shared and with whom it is being shared. To develop this language, communities must ensure that they are in compliance with Federal, State, and local privacy laws.

The client-agency written consent form serves as the initial authorization for inputting client information into the HMIS and governs all subsequent use of that information. Although an agency may have existing client consent forms documenting that a client has given consent to case managers to share confidential information with another agency's case manager, each agency needs to specifically request consent from each client to input the case management record and to subsequently share (anonymously or otherwise) that information. It is critical that the HMIS client consent form explicitly state how the data will be collected, shared, and used, and also the consent must explain a client's right to protect and limit its use (see sample consent form in appendix J).

- Interagency data sharing

The community's information-sharing philosophy and procedures should be clearly stated in the SOPS. The procedures should include a three-pronged strategy:

- Written client consent (as discussed above).
- Written interagency data sharing agreements between particular agencies as needed.

- Appropriate data security elements (discussed below, under security enforcement methods). Separate interagency data sharing agreements should be executed between the executive directors of specific agencies interested in exchanging client-identified data.

The agreement should document an agency's interest in interagency data sharing and commitment to abide by the defined privacy controls. The agreement should list the specific sections of HMIS data that will be shared. For example, some agencies may choose to share intake, residential history, and service records but not health information. To ensure that the agreement is effective, peer advocates can be enlisted to check that policies are being followed (see sample data sharing agreement in appendix H).

Developing partner agreements

Just as a community must develop privacy protection protocols, it is equally important to develop formal mechanisms for enforcing compliance among system partners. Consumer awareness of these security measures can reduce fears about entering information into the system. Several types of enforcement are listed below. Because individual behavior is unreliable, the technical solutions (discussed in Step Three) are the first line of protecting client privacy and safety. Therefore, most communities need to use a combination of these enforcement mechanisms with technical mechanisms to support each policy. Specific SOPs should describe each enforcement policy.

- Agency-system agreement

  One way of ensuring that agency partners are aware of specific policies, procedures, and responsibilities is to require each agency partner to enter into a formal agreement with the central HMIS coordinating entity. Responsibilities of both parties should be outlined in this agreement, especially regarding commitment of resources (e.g., staff, financial, training, technical assistance, standardized reports) and responsibilities (e.g., adherence to all policies and procedures, agreement to enter specified data, frequency of data entry and aggregation). Variations of this agreement, which should be included in the SOPS, can also be required for each HMIS user to ensure that all users agree to comply with the community's adopted policies and procedures (see sample form in appendix I).

- User agreement/request for access form

  A user agreement is an effective way to make sure that each potential HMIS user is exposed to the user-related policies and procedures. The agreement should provide a description of user-related policies, expectations of use, and penalties for misusing the HMIS. It is helpful for the format to require the potential HMIS user to initial or verify that they understand each policy and/or protocol individually. The agreement can double as a request for access or request for a password to be assigned to a particular individual. To reinforce awareness of the policies and security, password access can be limited to set periods of time, requiring re-certification every year or two. This process also provides a written record of authorized users. User agreements should not replace initial and ongoing user training (see sample form in appendix J).

Initial and ongoing partner training

Training is an important aspect of ensuring appropriate and valid everyday use of the HMIS. Directors of agencies sign agreements, but that knowledge may not always make its way to the front-line staff. A community can require each potential HMIS user to sign a user agreement prior to assigning that individual a password to access the HMIS. This agreement should still be supplemented by user training.

Mandatory training for all staff using the system is an excellent way to emphasize the most important policies and the reasons it is imperative that everyone safeguard the information. Ongoing training programs can also reinforce data-entry standards to support data validity and help all staff fully use the system to support consumers. Peer advocates can play a critical role in these trainings, reinforcing the importance of privacy protection protocols and teaching sensitive interview techniques (see the section on client interviews below). Additional training can be provided to specific groups of users to optimize their use of system features. Training can also be an important way to involve consumers. Training policies should be delineated in the SOPS.

Achieving Data Accuracy

An HMIS is designed to improve existing data-collection mechanisms, enabling communities to gain a better understanding of the characteristics and needs of local homeless populations. However, in order to ensure that HMIS data are accurate, communities must develop policies around the conduct of client interviews, consistency of data collection across different HMIS participants, data-entry features, and data checking mechanisms in the HMIS software. These mechanisms can also be laid out in the SOPs manual.

Client interviews

Data quality and accuracy is improved when client interviews are conducted in a respectful, sensitive, and confidential manner, which includes an explanation of HMIS goals. Consumer involvement in developing this process can offer an insider perspective on how questions should be asked and the timing of data collection. Consumers who have experienced intake procedures during a past or present shelter stay, can understand the discomfort of being asked invasive questions at a vulnerable time and can give insight into subtleties, such as tone of voice, eye contact, and timing, that might enhance or diminish their willingness to provide accurate data. Data accuracy will also improve if consumers receive direct benefits, such as benefits screening, when their data are entered into the HMIS.

Some current HMIS users report that collecting the required information on paper forms is preferable to entering data into the computer during the client interview. This method ensures that personal contact can be maintained when talking to consumers. Data can be entered into the HMIS later. However, other communities report that paper data collection and subsequent data entry contributes to data-entry barriers, particularly for programs that provide services to large numbers of clients each day. Hand-held computer devices, scanable intake forms, and consumer identification cards that can be swiped to record service activity may interfere less with personal relationships and ease data entry.

Community Example #6: Chattanooga, Tennessee

Service providers in Chattanooga, Tennessee, initially feared that using computers to enter data during the client interview might hamper the case manager-client relationship. Instead, they learned that using a paper form was inefficient and decreased time for case management. The case managers found that through training and familiarity with the HMIS software, they were able to maintain a sound clinical approach and ensure accurate data entry. As a result, clinical staff enter all data and the HMIS has replaced virtually all hard-copy information. Case managers input case management notes and other information immediately after the client therapy session thus ensuring that the HMIS is always up to date.

Consistency in data collection

As outlined in Step Two, all participants in the HMIS need to agree to a minimal standard of data elements that are feasible for collection by all. Some of these elements may vary by service population. For example, individual and family programs may all agree to collect basic demographic and historical data. However, family programs may also gather detailed employment and educational information, while individual shelters may not have access to these data. As long as there are enough data for reporting across the whole system, it is appropriate to report additional information for particular populations.

Programs and staff who collect the data need to share common definitions of each data element as well as collection points. For example, communities should agree on whether income figures are collected as monthly or annual amounts. Additionally, all participants need to gather the data at the same points in time. Referring to the income example, communities need to decide whether income amounts will be collected at program entry or some point during service receipt, exit, and/or follow up at a particular point in time (see Step Two for a discussion of data collection points). At the beginning of operation, the system manager should work with the software vendor to produce a data dictionary, which provides consistent definitions of all data fields.

It is critical to consistently assign a unique client identifier to each individual who provides information to the HMIS (see Step Three). This identifier will enable communities to create an unduplicated count of clients served by participating programs during a particular period. Individuals receiving services at different agencies will be identified and entered into the total count as one person.

Data entry

Training of data-entry staff is critical. In addition to explaining the use of the software, this training should stress the importance of accurate data entry, including procedures for double checking the data entered. Ideally, each site would identify a staff member with responsibility for regularly checking the accuracy of the data entered. This verification could be accomplished by checking all records against intake forms and other paperwork or by reviewing a random sample of all data entered.

Data accuracy will be greatly enhanced by having the same person who collects the information enter it into the HMIS. That way data-entry errors based on unclear information collected on the paper form can be avoided. When consumers and service providers receive a direct benefit from collecting and entering data in the HMIS, it promotes timely and careful attention to data collection and entry.

Community Example #7: State of Massachusetts—Outline of Standard Operating Procedures Manual

Section 1: Contractual Requirements and Roles defines the contract requirements of the central server and agency sites and the roles of central server staff, steering committee, and all participating site staff members.

Section 2: Participation Requirements identifies the specifications required for all participating sites and the central server. It also explains all of the contractual documents and requirements that relate to HMIS participation, including interagency data sharing agreements, written client consent procedure for electronic data sharing, confidentiality and informed consent, interview protocol, data collection commitment, information security protocols, connectivity, maintenance of onsite computer equipment, and conversion of legacy data.

Section 3: Training provides curriculum information, frequency, central server commitments, and optional training services.

Section 4: User, Location, Physical and Data Access specifies the security measures, including system access privileges, access levels, system location limitations, data encryption and storage, unique user IDs and passwords, and auditing procedures.

Section 5: Technical Support and System Availability details technical support services, availability, and performance commitments.

Section 6: Stages of Implementation explains the four stages of implementation, beginning with start-up paperwork and ending with full integration of the data system into program operation.

Section 7: Encryption Management specifies the encryption philosophy, approach, and decryption procedures.

Section 8: Data Release Protocols identifies the coverage specification, release authorization process, and right to deny access to client-identified and aggregate information.

Section 9: Internal Operating Procedures details the procedures that address the internal functions of a Web-based HMIS, such as prevention, detection and eradicating computer viruses; electronic internal communication; backup and recovery procedures; and the disaster recovery process.

Supporting Materials

- An annotated outline of Massachusetts' SOPs manual is available at http://www.mccormack.umb.edu/csp/csp_tech.htm.

- For an example of Standard Operating Procedures (SOPs) and related forms, the State of Wisconsin has established a Web site for their HMIS users that may provide a useful model for others. See http://www.doa.state.wi.us/dhir/boh/servicepoint.

- See the Appendices for the following:
  - Sample Client Information Sheet (appendix G).
  - Sample Interagency Sharing Form (appendix H).
  - Sample Agency Participation Agreement (appendix I).
  - Sample User Agreement (appendix J).