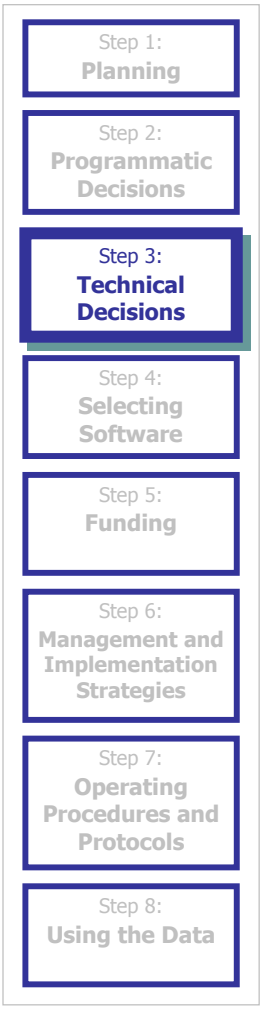
Step Three: Designing the System—Technical Decisions



The second part of the design process involves the formulation of technical decisions. Technical system features serve as a mechanism for implementing the community vision (Step One) and programmatic goals of the HMIS (Step Two). This step discusses the major technical design decisions, outlines the final steps required to articulate system requirements in preparation for Step Four: Selecting Software, and describes how a community can assess its current technical capacity. Finally, this step provides an example of an alternate approach to planning used in Spokane, Washington.

Major technical design decisions include:

- System scope.
- Structure and connectivity.
- Platform requirements.
- System security mechanisms.
- Other technology features.

All technical decisions should be documented throughout the process, adding to the system design requirements document begun in Step Two. This process will culminate in a report that details the existing technical environment and infrastructure recommendations to meet the technology needs of the proposed HMIS.

Step Three output:

- System Design Requirements Document—Part Two.
- Technical Infrastructure Assessment Report.

Technical Workgroup Role and Responsibilities

As with all of the earlier steps, the technical recommendations should be developed by an inclusive group. Depending on the size of the community, all of the primary stakeholders may participate in this group or a subset can be convened as the technical workgroup (as described in Step One). Although this workgroup should include individuals with technical expertise, it is also important to have continuity between the stakeholders involved in the programmatic design and this step. Often technical experts can be found among the staff of local service providers or local government. In some areas, community residents working with local technology firms may be willing to volunteer their time to participate in both this phase of the process and Step Four: Selecting Software.

The primary responsibilities of the technical workgroup are to develop technical system design recommendations and to assess existing technology infrastructure. These tasks are interrelated and can occur concurrently—each informing the other. For organizational simplicity, this step first describes the technical design decisions and then focuses on the technical assessment process and report.

System Scope

Based on the programmatic scope and size decisions, the technical workgroup can determine technical size specifications. The scope of the system is used to gauge the capacity needs of the central equipment and software and to provide a basis for estimating site equipment and software.

The technical scope statement should estimate the number of agencies and programs participating. For each agency, the following should be quantified:

- Staff positions that will be provided access to the system.
- Concurrent users (maximum number using the system at the same time).
- Seats (the computers on which the software will be accessed).
- Beds/service slots to be covered in the HMIS.
- Annual intakes (new clients who will be entered into the system during a year).
- Case management clients (new and active carry-over clients).

For I&R services, the scope information should also include the number of:

- Participating agencies supplying services along with their capacity, eligibility criteria, and service types.
- The frequency with which the information needs to be upgraded.
- Annual referral transactions per agency.

Structure

The structure of the system will vary based on the purpose of the HMIS, data sharing decisions, privacy policies, and existing systems already in place. Regardless of project scope and the specific goals for the system, the fundamental structure of all HMIS packages is based on the existence of a central place in which data are aggregated and stored—the central server or central data repository, which facilitates the electronic storage of aggregate or client-level data in one place to support service coordination and to facilitate reporting and analysis.

The two major options for system structure are *real-time* or *batch* systems. Other options combine both methodologies.

In a real-time system, all programs use the same software tool to enter client-level information into a central data repository. The central server can usually be accessed by a phone line (dial-up access) or over the Internet (continuous access). If a community wants to support real-time case management, program referrals, or any interagency data sharing, a centralized Web-based system structure is the best approach. Data aggregation, reporting, and system administration are all simplified with a real-time system. However, a real-time centralized structure presents greater security risks because all client data are stored in one database accessed by agencies. The security step of this step identifies security protections that can be used to mitigate risks to clients.

In a batch system, all users enter information on either their personal computer or local database application. The information is periodically uploaded (transferred in batches) to a central data repository. If a community does not want to use HMIS for any purpose other than periodic reporting, a batch system may meet its needs with lower security risks than a real-time system. However, because a batch system involves merging databases, access to current aggregate information can only happen when all program data are synchronized and sharing information among programs cannot occur unless individual programs

dial-up and communicate directly with one another. Merging databases also requires a high level of skills and coordination, impacting staffing needs (see Step Eight).

Regardless of the structure, some systems, especially those based on Web-enabled technology, offer the possibility of offloading the technical issues involved in organizing, setting up, and operating a central server to a third party. In such situations, a third party, such as the HMIS software vendor or local software service company, may provide hosting services. These services involve the technical administration of the HMIS and data repository, which will normally reside at the location of the hosting organization.

Connectivity

Connectivity—the way that agency site computers communicate with the central server—may vary depending on the selected structure. For real-time models, the Internet is the most effective means of connectivity because it minimizes software requirements at the site level. Using the Internet for this purpose avoids technical issues associated with installing software, fixing bugs, and providing other technical support at each site. These software challenges still need to be addressed on central server equipment. Alternatively, site computers can be configured to dial into the central server directly, without going through the Internet. However, this method is generally slower and more expensive than Internet alternatives. Another connectivity approach involves the use of emulation methods or multi-session environments, such as Citrix and Microsoft Terminal Services. These methods achieve real-time connectivity with or without the Internet. They run Microsoft Windows (rather than an Internet browser) applications over a network.

For periodically accessed models, dial-up access is the most secure approach. This method may reduce site connectivity costs. Site computers can be scheduled to dial into the system at a regular time, such as in the middle of the night once a month or as needed, to minimize tying up phone lines or computer time during the day.

Platform Requirements

Platform requirements refer to the specifications of the central system and server used for the central data repository. Platforms are also required for backup and recovery equipment at the central server organization and for equipment and connectivity at the agency site level. Different HMIS software packages use varying types of databases and require different equipment configurations, some of which are both less expensive and less robust, and others that are more expensive but able to accommodate sophisticated functioning more effectively. Although a community does not want to overbuy, particularly when technology and equipment design change so frequently, it is important to purchase a system that will grow with the community's needs thus minimizing the need for future overhauls. The systems requirement document can request that a vendor address specific plans for future development and enhancements.

Scalability

Scalability refers to the robustness of the system. Depending on the scope of the project and implementation strategy, a community may want to develop product specifications for a system that can handle large volumes of data quickly and reliably. These requirements include expansion capacity to meet local needs as the number of records increase and maintain the speed of data transmission from multiple sites.

For example, a statewide coordinated implementation strategy involving large numbers of programs with numerous client records should select a product that has the ability to scale to maintain system performance—even as new programs with large numbers of clients and staff begin to participate.

Flexibility

The platform that the HMIS database uses should have the flexibility to support basic user maintenance, such as user-defined data fields and updates to selections for drop-down menus. The database should also use industry standards that support the ability of the central database to interface with existing agency databases, including the capacity to customize conversion from one or more existing systems currently used by HMIS partners.

Again, there are tradeoffs between small and large database packages. Small database applications, such as Microsoft Access-based systems, may not be complex enough for aggregating HMIS data with appropriate security protections. Conversely, although more robust packages (e.g. SQL and Oracle) are definitely suitable, they require technical administration.

System Security Mechanisms

Designing and maintaining a secure system is essential to the ongoing use and integrity of the HMIS. Agency staff and consumers will not support the system if it fails to meet their security needs and contributes to client vulnerability. The privacy protection policies developed in Step Two should be enforced with technology mechanisms that limit behavior of system users to prohibit them from activity that might leave the system vulnerable. These types of security features primarily protect the system and client records from being accessed, changed, or shared by unauthorized users.

Security measures include:

- User accounts, passwords, and access protocols limit access to authorized users of the system. They can be used to limit which information particular users can view and/or revise based on defined access levels (read, write, edit, and delete specifications, variable by HMIS module).

- User agreements define appropriate and prohibited user behavior. In these agreements, users certify commitment to abide by HMIS policies and procedures (see Step Seven for more detail on these policies).

- User authentication verifies that a particular user is authorized to access the system.

- Location authentication verifies that the computer (location) is authorized to access the system. Possible options include public key infrastructure (e.g., certificate authority).

- Transaction audits track critical information on who, what, and when certain data are modified. The firewall, Web server, and central database can also be audited.

- Data storage protections protect data stored on the central server. Mechanisms include hardware and/or software firewalls.

- Data transfer mechanisms protect data while they are transferred from one location to another. Mechanisms include Secure Socket Layer (SSL) protection for over-the-wire transfer or for

decentralized systems, stripping client-identifying information, splitting identifiable data elements from sensitive, or protected data fields during transmission.

- Penetration testing checks the system for security weaknesses and failures and identifies vulnerabilities using contracted computer hackers on a regular basis.

- Back-up and disaster recovery procedures regularly create (secure) back-up data in case of loss or contamination of primary data. Offsite storage of back up data is recommended.

- Restricted equipment and data locations limit storage of equipment and data in locked and/or monitored locations, including back-up data storage files.

- Reporting Protocols can limit publication of information to anonymous aggregate client information with appropriate authorization by a local advisory group.

A Special Note on User Access: When the HMIS is established, a system of access needs to be determined. Some jurisdictions establish an access hierarchy in which the lowest level is read-only access. The next level might allow access to add and edit records. A third level might be established to add, edit, and delete records. A fourth level might allow the user to define access rights for other users within the organization and so on. Generally, the system administrator has the highest level of access. However, many systems will require a multi-step process with multiple users completing certain high security tasks, such as de-encryption of the database. In addition to type of access, stakeholders must determine which records particular types of users should be allowed to access. Even with read-only access, a single individual should not be given rights to view every record in the system, unless there is an overwhelming functional need to do so. More likely, each case manager should be given an appropriate level of access to the records within their program. If they work in multiple programs, perhaps the system can be coded so they can view only the cases that are assigned to them. Or they could be given access to both programs. The executive director or data analyst for the agency may be given rights to see all records for that agency, but that individual would not have access to other agencies' client records.

In some jurisdictions, the system administrator does not even have access to every agency's case files. These communities have decided to aggregate only anonymous data. Therefore, there is no access to systemwide identifiable client data.

It is important to remember that these security measures should be implemented in conjunction with the privacy protection policies defined in Step Two and standard operating procedures that will be defined in Step Seven, which clearly define client release/consent options for general HMIS participation and interagency data sharing, behavioral expectations of system users, and enforcement mechanisms.

When defining security mechanisms, a community should consider these related questions:

- What is the process for assigning and maintaining user accounts and passwords?

- How will physical workstation locations at participating agencies and central server equipment be secured?

- Is the database of client and service information secure at agency sites? Central server? Transmission between sites? Are there security protocols for each?

- How frequently and what information needs to be backed up? Under what circumstances would old data be retrieved?
- Who will host the data? Does the host meet the security policy? Contracting out for services may save the trouble of doing it inhouse, but local stakeholders are still responsibility for ensuring that the host has adequate security measures in place.

- What enforcement mechanisms and penalties will be established for people who violate system security?

Other Technology Features

The community should also consider whether other features should be incorporated into the technical design specifications. For example, in Step Two, minimum data standards were discussed. The community's data policy may suggest several technical requirements related to the unique client identifier, data fields, and additional technical features, such as data-entry error and omission queries.

System Design Requirements Document

At the culmination of the design process, all of the community decisions on program policy issues (Step Two) and technical design specifications (Step Three) should be formally documented in a systems design requirements document. This document will become the foundation for software solicitation and can be used by the community to develop evaluation criteria for gauging whether a potential software package is a good match with the community's needs. The systems design requirements document can be organized in a way that makes sense for the local community, but it should include at least the following:

- Size and scope (programmatic and technical specifications).
- Desired function.
- Data sharing policies.
- Privacy protection policies.
- Data requirements.
- Core business processes.
- System structure.
- Connectivity.
- Platform requirements.
- System security mechanisms.
- Other technology features.

This process may feel overwhelming, particularly for small jurisdictions in which one or two individuals may need to lay out all of the design options, make many of the decisions, and compile the requirements document. In some cases, it may make sense to seek out local MIS experts who can assist with parts of the process. In other cases, some of the issues can be considered simply and quickly, because there are fewer stakeholders and fewer options. Information for the technical infrastructure assessment can also be more easily obtained in areas with a small number of provider agencies.

Technical Infrastructure Assessment

Before selecting a software system or making decisions about system management needs, it is important to understand the community's existing technical capacity. A technical infrastructure assessment will identify the technical resources among provider agencies, government partners, and other HMIS participant organizations. The resulting report should provide recommendations on the specific equipment, desired functions of the software, and system management; serve as a companion to the system design requirements document; and facilitate cost estimating during Step Four and Step Six.

The technical workgroup should be responsible for conducting the assessment with the support of a staff person or designated workgroup member (referred to as the assessment administrator) to specifically manage the process. The assessment will be much more effective if all of the stakeholders understand its importance and if each agency/site assigns a staff contact to compile that site's information. Consumers can be involved in administrative tasks related to the technical assessment, such as conducting and tallying surveys, making follow up calls, or assisting in the arrangement of site visits or meetings.

The assessment should also be closely coordinated with other HMIS planning activities to ensure that the scope of agencies included in the survey effort is consistent with the scope and jurisdiction identified in Step Two. The technical workgroup should schedule assessment activities so as to complete the effort within a brief period of time.

Assessment objectives and process

At the beginning of the assessment, the technical workgroup should formulate assessment objectives and develop a rationale for the process that can be shared with agency administrators and site contacts. Common objectives include:

- To understand the existing capabilities of the network of agencies.
- To develop a sense of the willingness of service provider agencies to participate in the HMIS.
- To better understand system requirements for equipment, personnel, and training.
- To provide a basis for estimating costs.

The basic objectives can be accomplished using a detailed survey questionnaire complemented by several focus groups. The survey questionnaire should be designed to capture figures and objective indicators of processes and capacities. (A sample questionnaire is provided in appendix D.) The workgroup can conduct focus groups with site participants to probe the more subtle motivations and concerns of the many individuals whose business processes will be affected by the HMIS use. In particular, focus group exercises can inform site-training needs.

To complete the survey process, the assessment administrator needs to work with the technical workgroup and other planning committees to compile a complete list of potential HMIS participants and appropriate agency/site contact information. Once the survey is designed and approved by the technical workgroup (or higher level planning entity), the survey should be distributed to all of the participating agencies with a concrete deadline for responses. It is critical to get complete and accurate responses from all of the participating agencies. Therefore, the technical workgroup or assessment administrator should develop a plan to conduct calls and/or e-mails to request the return of completed surveys and to follow up on any missing or unclear information. Slow responses from agencies may indicate that these agencies are unaware of the process or are reluctant to participate, requiring additional outreach to increase buy-in. After the completed surveys have been returned and checked for errors and omissions, the responses should be compiled and analyzed. By comparing the assessment results with the technical design recommendations, technical infrastructure recommendations and requirements can be developed.

The six components of technical infrastructure

The technical assessment survey should be designed to acquire quantitative information about existing technical capacity and infrastructure in the following areas:

- Equipment: Information on the number of computer workstations in place, their characteristics and age, printing capacity, current connectivity (modems, phone lines, Internet access—e.g., phone, DSL, T-1 lines), and security features.

- Systems: Specific management information systems (MIS) currently in use at each site, including client-related case management, spreadsheets, financial or bookkeeping, reporting, and grants management software. Information about other software packages is also useful, including word processing and Internet applications.

- Data: Information about the methods that agencies use to analyze their data, including any manual or computer-based processes used to tally the numbers of clients served and outcomes of service delivery. Since most agencies use a combination of both manual and automated methods to organize their data for reporting and management purposes, exploring the categories of data that have already been automated, the specific database products used, and the length of time the agency has utilized this technology is important. This information will inform staff training and data conversion needs.

- Operational procedures: It is important to understand the major procedures and policies that participating agencies use related to the collection, manipulation, and sharing of client data. This portion of the assessment should produce specific lists and indicators of the particular policies and procedures. This information can be used to inform the development of standard operation procedures, staff training, and data integrity and security mechanisms.

- Organization: Information about each agency's services, listing the primary characteristics, bed count or case management capacity, annual client capacity, and number of staff by type for each unit of activity. The survey should clearly define a unit of *activity* to ensure that agencies and programs respond consistently. For instance, a unit of activity can be defined as an agency, a program, or a site (physical location). These units of activity will be used to identify software license and equipment needs and data capacity estimates and to distinguish them for reporting and security purposes. For example, if an emergency shelter program and transitional program operate at the same site, it may be helpful to distinguish programs for reporting purposes. Most emergency shelter programs have different reporting requirements, varying expectations of client outcomes and, follow-up case management protocols. Therefore, the system needs to differentiate between the two programs. However, if the programs are reported separately but are staffed by the same case managers, the level of staffing overlap should be indicated on the survey so an accurate number of staff user licenses can be calculated. Similarly, if one program has multiple sites, the locations should be indicated so an accurate equipment estimate can be generated.

- Skills: Information on the level of site staff competence and expertise in information and computer systems. The survey should request specific information on the numbers of staff that fall into various categories of expertise, including basic exposure to computers and networking; use of computer productivity tools, such as word processing and spreadsheet tools; and use of business-specific computer applications, such as case management or program management products. This information will be used to design appropriate training recommendations and to identify staff members within participating agencies who can be engaged in a more prominent role in HMIS implementation project because of their expertise.

Defining infrastructure requirements

There are three major steps involved in the preparation of the infrastructure recommendation. A master spreadsheet with the site information from the survey assessment may help organize the various equipment, staff, and training needs for the central organization and each individual site. In addition to the areas described below, some specific cost items are discussed in Step Five. Detailed information can be found in the HMIS Cost Estimation Guide (see supporting materials at the end of this step).

- Estimating equipment and license requirements

  Equipment and license requirements can be estimated from the agency survey assessment. These estimates will vary based on system-function decisions, system structure, and connectivity decisions as well as business processes, all of which should be included in the system design requirements document. The agency survey should provide the total number of computer users (program, data entry, and administrative staff who will access the system) and the number of sites that will be connected.

  The number of personnel, numbers of clients served, and the business processes will determine the number of computers required. For example, if the HMIS is used directly by client and case manager for I&R or benefits screening, each staff member may need a computer. However, if the HMIS is used only for reporting purposes and an individual administrative staff member inputs the data, fewer computers may be required. Also, in the estimation phase, the workgroup should consider the level of need for printers, modems, or other connection devices; communication lines; and such equipment as scanners and/or digital cameras to post pictures or print identification cards. The central organization equipment estimates will vary depending on community requirements. For example, if the community wants to incorporate an I&R component in the HMIS, the central organization will need additional database development, maintenance, storage, connectivity, firewalls, and security capabilities. Similarly, an Internet-accessible central server may require equipment and software different from a dial-up, periodically accessed system.

  The total number of software licenses or copies needed will depend on staff levels, roles, work schedules, and proposed business processes. Vendors of HMIS products define user licenses differently from other software producers. Some licenses are based on seat while others are based on individual user names and passwords. Software licensing for the central server should also be calculated. Depending on how the software is installed and accessed, the central server licensing may vary. However, generally, the vendor will issue one central server license and multiple client licenses.

  Whether an agency can use concurrent licensing is a prime factor. Concurrent licensing allows staff members to share a license when one staff person will not be using the system at the same time as others; each user maintains individual access passwords and protections. Licenses may be shared when, for example, an agency employs 50 case managers on 3 shifts. If no more than 20 staff would ever be logged on at the same time, the agency could purchase 20 licenses with 50 user accounts. In this type of setup, if all 50 staff were to come to work for a special meeting one day, no more than 20 could be logged on at the same time.

- Identifying staffing and service needs

  To be successful the HMIS initiative will require staffing. Most of the staffing requirements will be for the organization that manages central operations, such as project management, system

administration, agency coordination and technical assistance, data administration, reporting, and training. In some instances, a community may prefer to contract certain services with third parties. The system management roles and options are described in greater detail in the management models step of Step Six. However, many of the initial requirements need to be identified at this point in the process.

Agencies will also have increased staffing needs to complete client interviews and data entry as well as to manage and maintain site-specific hardware and software.

- Identifying training needs

  To successfully implement and operate an HMIS, establishment of an ongoing mechanism for developing skills and ensuring that these skills are used is essential. Without training and quality control measures, the entire initiative will be in jeopardy. The system could be put in place, but never used. Staff could enter data that are so inaccurate they cannot be aggregated. Client privacy and security could be at risk.

  Based on the HMIS function and design, the workgroup should produce job descriptions for both central organization and site staff. The technical skill base should include a description of skills needed for each type of staff position, such as the required understanding and proficiency in:

  - Computer operating systems.
  - Computer networking.
  - Internet operations.
  - Database applications.
  - Use of e-mail and other productivity tools.
  - Basic interaction with computers.
  - Operation of the specific HMIS application, including basic functions, appropriate use of security mechanisms, and standard operating procedures.
  - System administration functions.

  Then, based on a comparison of the technical skill base with the assessment of existing staff expertise, the workgroup can develop the format, frequency, and cost of delivering training to broaden the base of technical skills. The workgroup may also determine whether current staff can conduct training or if there is a need to hire a local TA consultant, the HMIS software vendor, and/or a combination of these options.

Developing the technical infrastructure recommendations

The final step of the technical infrastructure assessment process is to prepare the Technical Infrastructure Recommendations document that identifies the basic elements necessary for the HMIS cost estimation. It may be organized by the central-organization and individual site needs:

- Central organization information: equipment, software, services, and staff (positions and professional services).

- Site information: type of program or agency, clients served, equipment, and staff (positions and training), individually itemized for each agency or unit of activity.

The final report should compare the analysis of the existing technical infrastructure with the needs of the proposed HMIS, designed in steps Two and Three. The final report should highlight the extent to which

the HMIS can rely on existing equipment, software, and staff, and should specifically identify the equipment, systems, staff, and training that need to be acquired for a successful HMIS implementation. This information can be used by software vendors to develop their cost estimates, by the technical workgroup to evaluate software proposals, and by implementation workgroups to purchase equipment and make system-management decisions.

Alternative Approaches to Planning and Implementation

Although this guide outlines the HMIS planning and implementation process in a linear eight-step process, in reality planning is more likely to be iterative—the community learns from each step of the process and decisions made early on may be revisited later in the process. Rather than using a linear step-by-step process, there are communities that have been successful at merging the design and implementation processes. Spokane, Washington, is an example. Spokane decided to design its own system in-house to make the most of limited time.

Community Example #5: Spokane, Washington—An Alternative Approach to Planning and Implementation

To design a system quickly and in a hostile environment, Spokane adapted a best practices software design model called Rapid Application Development. This model uses a prototyping methodology—a conference room pilot. The conference room pilot worked with a select group of providers who deliberated HMIS planning issues and concurrently developed and ran a prototype HMIS. Thus, the planning and implementation processes were intertwined, each informing the other along the way.

This approach was selected because most stakeholders either had little experience with automation or a history of automation/measurement failures. Some had participated in State-driven data collection and aggregating efforts that had either returned no information or generated error-ridden reports. The conference room pilot model allowed participants not only to better understand the implications of critical path decisions but also to begin to develop trust in the overall measurement process. This process also allowed Spokane to work out many implementation problems and concerns within a smaller, less complex environment, reducing the likelihood of a large and costly failure. Finally, this pilot approach also created a core group of knowledgeable users who took ownership and sold it to other community programs.

The process began by identifying a few providers that were willing to participate in the prototype development. Four organizations, representing larger area providers and local leaders, assigned both directors and line staff to participate in the planning process. This group initially answered critical questions. Although one homeless consumer was included in the group, client representation was weak.

The group conducted the following activities:

1. Identification of consultants, including a measurement specialist with extensive history in social service databases, an information technology (IT) person, and a legal aid, to support the group.

2. Definition of the initial objectives and core values for the proposed system: What was absolutely needed from the system? What would be nice but not necessary? What functions could be supported over time?

3. Identification of privacy and security constraints along with a variety of strategies for solving them. This discussion focused on whether interagency-shared client-level data was feasible or meaningful enough to offset the inherent risks. An initial client identifier strategy was also developed.

4. Completion of a technical infrastructure assessment with the initial list of potential participants.

5. Review of an existing specialized software package. Stakeholders also reviewed the risks and assets of developing a homegrown system. Budget and function were critical to this discussion. The group decided to go with the homegrown approach. This decision was driven by experience with vendor failures as well and a low overall project budget.

6. Decisions about platform and a myriad of other technical issues with the support from the IT consultant.

7. Identification of the initial data elements based on existing intake, assessment, and discharge forms as well as a review of typical Federal, State, local, and private-funder requirements.

8. Formalizing of processes for data storage and transfer among sites.

Throughout this stage of the development, group members reported initial decisions and talking points to the larger homeless coalition on a monthly basis. Coalition input was integrated into the small group discussions.

The IT consultant developed an initial prototype and the four organizations began to use it. The consultant was flexible with data element design and redesign. Reports were produced for the coalition to demonstrate the power of the information and reduce anxiety. These presentations were coupled with training on methods for defining and measuring outcomes and use of database information to improve organizational level planning and operation.

By the end of the first year, Spokane had been through several permutations of the data elements that would be included in core reports as well as the information to populate those fields. Through this interactive process, the group stabilized the core fields and procedures for entry, storage, and reporting. Other organizations then joined the system. The number interested in participating grew substantially during the second year—and has grown every year since. Currently, the project includes shelters, transitional housing providers, and feeding programs, mental health outreach teams that canvas people living in the rough, domestic violence shelters and court programs, and the Spokane School District. Shared communitywide outcomes have been defined and are used to report to a diversity of funding sources at both the agency level and across the total continuum of homeless providers.

The group members added an ongoing design/redesign process to the database project, which they believe is key to its survival. Membership in the ongoing process is open to all participants. Each year, members review data elements for relevancy and data integrity, discuss definitions, revise procedures for collection and dissemination of information, review proposed new data elements, and discuss confidentiality. Core values identified during the implementation stage, including flexibility, relevance, data integrity, feedback, collaboration, and trustworthiness, continue to guide the evolution of the project.

Supporting Materials

- See appendix B for a sample security layout.

- *Safe Harbors Design Project,* prepared for the City of Seattle, King County and the United Way of King County (February, 2001). See pages 9 to 27 for a detailed description and graphic layouts of the systems' three levels. This publication is available on HUD's HMIS Web site at http://www.hud.gov/offices/cpd/homeless/hmis/index.cfm.

- *Homeless Management Information Systems: An In-Depth Look,* Center for Social Policy, McCormack Institute, University of Massachusetts-Boston (January, 2001). See pages 13 to 16 for information on system structure. This publication is available on HUD's HMIS Web site at http://www.hud.gov/offices/cpd/homeless/hmis/index.cfm.

- *Homeless Management Information Systems (HMIS) Cost Estimation Guidelines: Cost Framework and Submission Recommendations,* Center for Social Policy, McCormack Institute, University of Massachusetts-Boston/Aspen Systems, Inc. (January, 2002). Document provides detailed information on technical cost elements. The publications is available on HUD's HMIS Web site at http://www.hud.gov/offices/cpd/homeless/hmis/index.cfm.

Technical Design Exercise #1: System Structure Working Group

Questions to Explore:

1. How will the system be structured?

2. What is the current technical capacity within each continuum area for HMIS adoption?

3. What software tool(s) will best meet the needs of the system?

4. Who will be responsible for the central administration of the system?

5. What are the base requirements at each level (State, community, agency) for:

   - Hardware.
   - Software.
   - Staffing/personnel.
   - Training.
   - Technical assistance.

Resources for Working Group:

- *Homeless Management Information Systems: An In-Depth Look.*
- *Homeless Management Information Systems (HMIS) Cost Estimation Guidelines.*
- *Homeless Service Tracking and System Implementation Guide.*
- *Safe Harbors Design Project.*

Technical Design Exercise #2: System Structure

Questions

Based on your community's purpose statement and identified goals, create subcommittees to address each of the four issues below. Choose one topic from the list and prepare a response to the questions for the next HMIS planning committee meeting.

A) System functions: Despite preparation of a purpose statement, questions remain about the structure of the system. What system structure do you recommend? Using the structure you select, what types of information will be gathered and how can they be used? What limitations do the selected structures impose?

B) System benefits: Service providers are interested in how the proposed system will benefit them and their clients. Funders, who are also interested in benefits to clients, will want to know that their money is invested soundly and that the project includes measurable outcomes. Please list anticipated benefits and outcomes of the system that will appeal to each group.

C) Existing systems: How will the new system accommodate those agencies in your community that already have databases? If those agencies are satisfied with their existing system, will the HMIS partners try to leverage the other agencies' participation in the community HMIS? Are there other ways to aggregate data from existing systems with the information in the HMIS to ensure an unduplicated count?

D) System administration: What type of agency would best serve as the central organization? How will the selection be made? Will the community seek to keep all system administration and project management functions internal or will outsourcing be considered? If so, for which functions?