Chapter One: HMIS Technology Elements and Architecture Options

Implementation of HMIS solutions requires sophisticated technological infrastructures. This chapter provides an explanation of the key technological concepts and terms relevant to the solution reviews in Chapter Three and subsections of Chapter Four. The chapter describes technological architecture including software, hardware, user interfaces, database locations, and hosting options. It concludes with a description of technological security mechanisms.

Key Technology Concepts and Terms

Computer-related Office Technology

Computer-related office technology can be grouped into two categories: software and information technology (IT) hardware.

The two main types of software are:

> *Desktop software:* Desktop software includes word processing applications, spreadsheets packages, presentation software, email applications, and Internet browsers.
>
> *Information management software:* This software is used to manage operations that include data stored in a database. These products can handle multiple users running the same application at one time. HMIS solutions are a type of information management software.

IT hardware includes:

> *Computers:* Computer hardware refers to personal computers (PCs), servers, and older mainframe computers.
>
> *Peripherals:* Printers and scanners are examples of peripheral devices.
>
> *Networking components:* Network components include routers, hubs, and cables.
>
> *Storage:* Storage devices include network disk drives and storage area networks.
>
> *Connectivity:* Connectivity includes Internet access over a T1, DSL, cable modem, or phone line.

Individual solutions will rarely meet all office technology needs. However, many providers have bundled their solutions with various combinations of software and IT to support community and agency requirements.

Information Management Solution Components

Information management solutions consist of three main components:

> *User interface:* The part of the software with which the user interacts is called the user interface. The user interface presents data and text on the screen and responds to user keystrokes and mouse clicks.

Application: The application processes all of the program functions, such as validating the integrity of the data entered by a user or generating reports.

Database: The database is the component that will record, store, and manage the data that the users enter into the application through the user interface.

Solution Architecture

Solution architecture refers to configuration of the solution components – user interface, application, and database.

Stand-alone (one-tier) architecture: When all three components operate on a single computer, solutions are referred to as "stand-alone" or "one-tier". Many HMIS solution providers offer a stand-alone version of their solution. Because it will not accommodate data sharing across agencies, this model is generally not considered an HMIS unless the community has only one homeless service provider or one point of data entry, such as in the case of centralized client intake and follow-up. When stand-alone models are used within a community setting, some degree of data aggregation can be achieved if each user of a stand-alone system exports data to a central repository. However, this aggregation is not automated and is difficult to accomplish.

Networked (multi-tier) architecture: In information management software, the user interface and the database usually run on separate computers in separate geographic locations that are connected via a network or the Internet. The database is centralized and the user interface operates on each user's computer. The application component can either be combined with the user interface or can run on a central server.

Networked architecture can be further subdivided:

Client/Server (two-tier) architecture: The application is combined with the user interface and both run on the user's computer that is referred to as a client computer. The database runs on a server in a central location.

Three-tier architecture: In "three-tier" architecture each component is distinct. Generally the application and the database reside on separate servers in the same geographic location. The user interface is located on each user's computer and merely provides a means of accessing the application. Solutions that use a web browser are examples of three-tiered architecture; the web browser serves as the user interface that enables access to both the application and database, which run at another location.

Architecture and IT Hardware Considerations

Solution architecture has implications for IT hardware decisions. In stand-alone and client/server environments, each user's computer runs all or part of the application; therefore, these computers should be reasonably powerful. These setups require that software be installed and updated via "patches" directly on each client PC. A patch is a small program that updates or fixes a previously installed application. In three-tier environments, the central servers do almost all the work, transferring everything the user needs across the network and the Internet. Therefore, the central servers should be powerful, and network or Internet connections fast and reliable; users' personal computers do not need to be as up-to-date. In this architecture, any updates to the solution occur at the central server location and are immediately available to all users. The actual performance of a solution is affected by the architecture and by the design of each

software component. The "Environment Scores" section of Chapter Four reports solution performance on various user computer configurations.

Network Architecture Implementation Options

Communities that choose to implement a networked, multi-tiered solution must make decisions in three areas: user interface, database location, and hosting.

User Interface

Three types of user interfaces are available for HMISs:

Client: Software written as part of the HMIS is installed directly on each user's computer. In a client/server application, the client combines the entire application with the user interface. In some instances, a client is used in a three-tier solution and some parts of the application are combined with the user interface; other aspects of the application are run on the server.

Web browser: Users of the HMIS access the application by using a web browser such as Netscape or Internet Explorer.

Remote interface: In this three-tiered model, a remote access program is installed on each user's computer, instead of the HMIS application. The program enabling remote access can either be "plugged-in" to a web browser or exist as a separate application. Many HMISs implement this model using Citrix, a third party application designed for this purpose. Rather than installing the actual HMIS application on each computer, each user installs Citrix.

Table 2: User Interface Options

Option	Description	Considerations
Client	The HMIS is installed and run directly on each user's computer.	- Application can be sophisticated and fast. - Requires installation and administration. Harder to implement upgrades. All users must use a vendor supported operating system; e.g., OS10, Linux, or Windows 2000.
Web Browser	User accesses the application by navigating to a website using a web browser such as Internet Explorer or Netscape.	- No installation or client upgrades. - Application functionality limited to the capabilities of the browser.
Remote Interface	The HMIS application is stored on a server. Another program is installed on each user's computer, which allows the user to access the HMIS application remotely. The program enabling remote access can be "plugged-in" to the browser or exist as a separate application.	- Initial installation needed. - No upgrades to user computers when HMIS changes. - Application can be sophisticated and fast. - Sometimes difficult to integrate the application into local functions such as printing.

Database Location

Networked systems employ two standard options for database location:

Centralized database: A centralized database stores all of the data in one central location. Users connect to the central database when they log onto the HMIS application. Data are not stored locally; users access the database only by connecting to the central server. While the user remains logged on to the system, requests to retrieve, update or remove data from the database take effect immediately. The centralized system allows for smooth data sharing across agencies. Keeping data up-to-date does not require a distinct administrative task.

Distributed database: In a distributed database model, data are stored locally at each data entry or program site. The various local databases are also replicated at a central location. Some HMISs perform the data replication process automatically at predetermined times. Others require agencies to connect to the central location to upload a copy of their database. Because the data are stored locally, the user can access the information for their site at all times. However, aggregate data reports are only as current as the data that have been transferred to the central data repository. The distributed database model can be faster because the local database only includes information specific to the user's agency and the application does not have to access the Internet to retrieve the data.

Table 3: Database Location Options

Option	Description	Considerations
Centralized	One database shared by all users at the same time.	- Enables data sharing across agencies. - All data is up-to-date. - Application speed depends on type of Internet or network connection.
Distributed (with replication)	There is one central database, plus each location has a distinct copy of the database. Each local database is periodically copied (replicated) to the central database using an automated process.	- General application does not depend on type of Internet connection nor by central server availability. - Can be faster than centralized system. - Often difficult to ensure that all data are up-to date. - Data aggregation for periodic reporting only. No inter-agency data sharing function.

Hosting

Hosting options for administering the database (and in three-tiered architecture, the application server) include:

Lead Agency Hosting: The community purchases a license from the solution provider to use the application and directly administers, or hosts, all components of the multi-tiered solution. The community, or one local partner (the "lead agency"), owns and configures the servers and the database system, then installs the HMIS database and application on the servers. The solution provider develops upgrades to the database and the application, but the lead agency is responsible for putting those upgrades on the central server. The lead agency licensing approach suits a

community that wants complete control of its own HMIS and has the necessary staff to administer it.

Third party hosting: The community purchases a license from the solution provider to use the application and then hires a third party to administer the application server and database. The third party can be a government agency, a non-profit, a corporation, or a local university. Often third parties can provide local expertise, security, administration, training, and support beyond the capacity of either the partners or the provider; however, they may also add to the overall project cost.

Application Service Provision (ASP): The solution provider hosts and administers the central database and application server. In some cases, the community purchases the actual server equipment that the provider hosts at its secure location; in other cases, the community uses the solution provider's servers. Communities that lack the capacity or desire to maintain the hardware and software for the HMIS should consider an ASP.

The decision to use an ASP or third party hosting model also relates to the hardware considerations associated with system architecture.

Table 4: Hosting Options

Option	Description	Considerations
Lead Agency Hosting (Licensing)	Community acquires a license from the software vendor to use the application. The database is administered by the lead agency - one of the community partners.	- Lead agency has direct control over data and server configuration. - May hire agency staff to administer or out-source IT administration.
Third Party Hosting (Licensing)	Community purchases a license from the software vendor to use the application, and then hires a third party to administer the application server and database. The third party can be a government agency, a non-profit, a corporation, or a local university.	- Third party can provide local expertise, administration, training, and support beyond the capacity of either partners or provider. - Agency does not need to hire staff to administer network. - Access to server and data controlled by third party, but overseen by partners. - Cost to provider based on licensing model, fee for service paid to third party instead of provider.
Application Service Provision (ASP) (Solution Provider)	The solution provider administers the central database. In some cases, the community owns the actual server equipment that the provider administers; in other cases, the community uses the provider's servers.	- Agency does not need to hire staff to maintain the HMIS hardware and software. - Access to server and data regulated by provider. - Fees for hosting determined by provider.

The various options for the user interface, database location, and hosting can be combined in multiple ways to create many distinct implementation models, though an individual solution provider may only support a limited number of approaches.

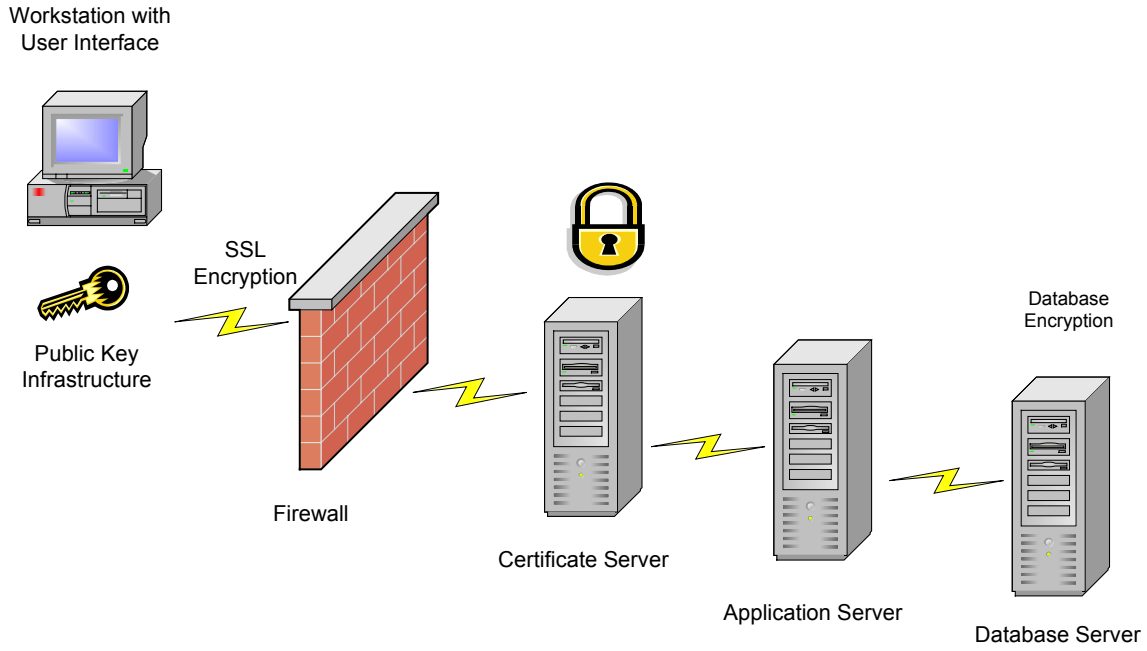
Security Configurations

In addition to the technological infrastructure, security mechanisms to protect client-specific information are an important part of the technology environment. Security concepts are referred to throughout this guide, but they are particularly relevant to the Data Sharing and Security section of each solution review in Chapter Three and the corresponding section in Chapter Four.

The commonly used security mechanisms described here are the technological solutions that increase system security. Standard operating policies and procedures should also be developed to ensure compliance with access protocols and client consent procedures.[6]

Figure 1 (below) displays an Internet based security model with several layers of security: a public key infrastructure and Secure Socket Layer (SSL); a firewall; a certificate server; an application server; and a database server with encryption.

Figure 1: Internet Based Security Model



[6] These policy issues are discussed in detail in the *Homeless Management Information Systems: Implementation Guide*.

Encryption

Plain text is converted into encrypted data by scrambling it using a secret code that masks the meaning of the data to any unauthorized viewer. Computers encrypt data by using algorithms or formulas. Encrypted data are not readable unless they are converted back into plain text via decryption, which prevents unauthorized persons from associating sensitive personal information with the identity of specific individuals. Two kinds of encryption are commonly used in HMIS implementations.

Secure Sockets Layer (SSL): A communications protocol used to secure all sensitive data. SSL is normally described as wrapping an encrypted, or coded, envelope around data transmissions when they are transmitted over the Internet.

Database: Encryption that occurs at the field (data element) level within a record of information.

Public Key Infrastructure

Public key infrastructure protects against unauthorized access to servers and/or data through use of a certificate authority. A certificate authority only allows computers with registered certificates to access the server and/or database. Two options for implementing a public key infrastructure include:

Self issued certificate authority: Most commonly used between parties that trust each other. Example: Microsoft Certification Authority.

Third party certificate authority: Most commonly used between parties that do not have historically trusting relationship. Example: Verisign.

Firewall

A firewall is a hardware and/or software system that enforces access control policies between two networks, usually between a Local Area Network (LAN) and the Internet. A firewall allows only specific kinds of information to flow in and out of the local network. This protects the computers and data on the LAN from intruders or hackers who might try to use the Internet to break into those systems.

Audit Trail

An audit trail is produced by an extensive auditing system that monitors, records and reports on the actions of valid users of the HMIS. This technology allows system administrators to monitor activity within the HMIS.