



HMIS Security & Confidentiality

Introduction

The security and confidentiality of homeless client personal information in a Homeless Management Information System (HMIS) is a major issue. For certain providers and sub-populations, such as Domestic Violence shelters, HOPWA shelters, and substance abuse facilities, security & confidentiality of client information becomes even a much larger concern. Extensive technical and procedural measures have been implemented by the Rural Arizona Continuum of Care to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosure of data.

HUD Privacy & Security Standards

The Homeless Management Information Systems (HMIS) Data and Technical Standards Notice, published July 30, 2004 by the U.S. Department of Housing and Urban Development (HUD), included extensive HMIS Privacy and Security Standards to be followed by Continuums of Care, homeless assistance providers, and HMIS software companies. These standards were developed after careful review of the Health Insurance Portability and Accountability Act (HIPAA) standards for securing and protecting patient information. The Rural Arizona Continuum of Care has and will continue to implement and monitor our practices and procedures to be in compliance with these Privacy & Security Standards.

Security & Confidentiality Policies and Procedures

In addition to the technical measures described below, the Rural Arizona Continuum of Care has implemented a number of policies and procedures to enhance security & confidentiality. Each agency that participates in the HMIS implementation must execute a 14 page Agency Partnership Agreement with the Arizona Department of Housing. This Agency Partnership Agreement specifies the responsibilities of all parties and includes security & confidentiality agreements. Each user, prior to being issued a user ID and password, must read and sign a User Code of Ethics forms that details their responsibilities for keeping client information confidential. Clients must provide consent to allow the entry of their basic information into the system. If client information is to be shared between two or more agencies, clients must sign a Release of Information form specifying which agencies may view their information and for what purpose. Procedures are also in place for securing hardcopy documents such as forms and reports. In addition, the system provides an audit trail of all attempted access violations that is monitored regularly by the system administrators.

System Security

The Rural Arizona Continuum of Care uses the ServicePoint HMIS software from Bowman Systems. As an Internet-based software solution, the HMIS software and databases are hosted on servers located at Bowman Systems in Shreveport, Louisiana. The servers are located in a highly secure computer room accessible only by a very few employees of Bowman Systems who are responsible for supporting and maintaining the servers. The computers are also protected by firewalls to prevent unauthorized external access.

User Authentication

As an Internet-based software system, each Rural Arizona HMIS user accesses the system via their Internet web browser (Microsoft Internet Explorer). To access the HMIS, each user must know the web address (URL) for the Rural Arizona version of ServicePoint. This web address is not published outside of the Rural Arizona Continuum of Care and is not available through web search engines. Once at the initial login page, the user must enter a valid user ID and password combination. A unique user ID is assigned to each user by the HMIS System Administrator. Each user must have their own user ID and password and sharing is strictly forbidden. Each password must be a minimum of 8 characters in length and must contain 2 or more digits (to prevent the use of common words). Every 45 days, each password must be changed. If an incorrect password is entered 4 times in a row, the user ID is disabled and the user is locked out of the system until it can be reset by the HMIS System Administrator. Passwords are always encrypted and can never be seen in clear text.



Rural Arizona HMIS Project

Encryption

Because all of the HMIS transactions travel over the Internet, all data is fully encrypted using Secure Socket Layers (SSL) with 128 bit-encryption. The 128-bit encryption is the highest level of encryption commercially available and is the same used by banks, online stores, and other secure web sites. Thus, all data from each user's workstation is encrypted, transforming it to unreadable characters from their workstation, is transmitted over the Internet, and then is unencrypted by the ServicePoint servers.

Application Security

The ServicePoint software also has a built-in security system that ensures each user only has the minimum access needed to do their job. Each user is given a security authority level in their user profile that grants access to certain system functions. Several different security authority levels are available, such as Executive Director, Agency Administrator, Case Manager I, Case Manager II, Agency Staff, Volunteer, etc. So within an agency, an agency staff person that just performs intake functions cannot see other information about a client, such as medical assessments and case notes, that a case manager could see.

Confidentiality – Closed Profiles

In the ServicePoint HMIS, by default, all client records are "Closed." When a client record is closed, only authorized users from the agency that created the record may view the client information. Users from any other agency cannot view any of the client information. It is also possible to enter clients as "Anonymous" or you can use proxy or coded names. However, leaving the profiles closed or entering clients as Anonymous or using proxy or coded names all can lead to the duplication of clients in the system.

Confidentiality – Open Profiles

If the client provides consent by signing a "Client Acknowledgement of Data Entry into HMIS" form, you can open up limited information in their profiles, typically just the name, social security number, and age. Thus, users from other agencies could see that the client is already entered into the system. However, they cannot ever tell that the client was at your specific agency or when they were there. User from other agencies would only know that, at some time, the client has been at some homeless provider in the Rural Arizona Continuum. Since opening profiles helps prevent the duplicate entry of clients but only opens very limited information, it is the recommended setting.

Confidentiality – Data Sharing Between Agencies

If you are working cooperatively with another provider or group of providers on a client and the client provides a signed Release of Information (ROI), you may be able to share additional data with only that provider or group of providers. You explicitly authorize, based on the client's release, what data can be shared and with which agencies. Data sharing between agencies can be for a limited time and can be revoked anytime.

Confidentiality – Reporting

Any reports generated for the CoC, HUD, and any other federal or state government agencies only includes aggregate, de-identified data. No identifiable client data, such as name, SS#, DOB, etc. is ever reported outside of the system.

Provisions for Domestic Violence Providers

In 2006, the Violence Against Women Act (VAWA) was signed into law. Among other topics, it did include provisions that disallowed domestic violence providers from entering client data into a system such as HMIS. As a result, all DV providers previously using HMIS were required to quit using HMIS and no new DV providers could use HMIS.

Summary

All parties – users, agencies, ADOH, Symmetric Solutions, Bowman Systems – take security & confidentiality very seriously. Violation of security & confidentiality is against the law. The Rural Arizona Continuum of Care has implemented extensive technical & procedural measures to protect client data.