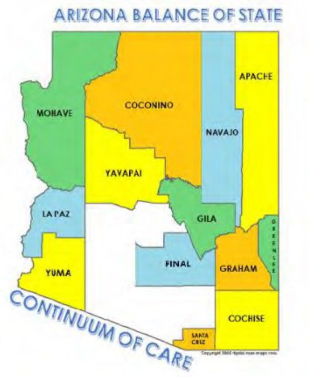
ADOH Arizona Department of Housing

Collaborative Applicant and Unified Funding Agency



Arizona Balance of State Continuum of Care HMIS Security & Confidentiality

Revised: March 5, 2024

1110 West Washington Street, Suite 280 | Phoenix, AZ 85007
Telephone: (602) 771-1000 | Facsimile: (602) 771-1002 | TTY: (602) 771-1001

EQUAL HOUSING OPPORTUNITY

HMIS Security & Confidentiality

Introduction

The security and confidentiality of homeless client personal information in a Homeless Management Information System (HMIS) is of utmost importance. For certain providers and sub-populations, such as Domestic Violence shelters, HOPWA shelters, and substance abuse facilities, security & confidentiality of client information becomes an even larger concern. Extensive technical and procedural measures have been implemented by the Arizona Balance of State Continuum of Care (AZBOSCOC) 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 (CoCs), homeless assistance providers, and HMIS software companies. The policies and practices in this notice cover the processing of protected personal information for clients of the AZBOSCOC. This notice covers personal information and data collected and entered into the AZBOSCOC HMIS. It does not apply to medical records or information covered by the Health Insurance Portability and Accountability Act (HIPAA) or other legal protections. These standards were developed after careful review of the HIPAA standards for securing and protecting patient information. The AZBOSCOC has and will continue to implement and monitor practices and procedures that are in compliance with these Privacy & Security Standards.

Security & Confidentiality Policies and Procedures

In addition to the technical measures described below, the AZBOSCOC has implemented a number of policies and procedures to enhance security & confidentiality. Each agency that participates in the HMIS implementation must execute an Agency Partnership Agreement with the Arizona Department of Housing (ADOH). 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 form that details their responsibilities for keeping client information confidential. Clients must sign a Release of Information (ROI) form acknowledging that their information is in HMIS and indicating whether they want their information shared with other providers. Procedures are also in place for securing hard-copy documents (e.g. ADOH Partnership agreement/Point of Contact/New User Agreements and the SAP Business Objects reports)- see the HMIS Policies and Procedures located at https://housing.az.gov/documents-links/forms/special-needs-continuum. In addition, the system provides an audit trail of all attempted access violations that is monitored regularly by the system administrators.

System Security
The AZBOSCOC uses the ServicePoint HMIS software from Wellsky Corporation. As an internet-based software solution, the HMIS software and databases are hosted on servers located at Wellsky Corporation in Lenexa, Kansas. The servers are located in a highly secure computer room accessible only by a very few employees of Wellsky Corporation 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 AZBOSCOC HMIS user accesses the system via their internet web browser. To access the HMIS, each user must know the web address (URL) for the AZBOSCOC version of ServicePoint. This web address is not published outside of the AZBOSCOC and is not available through web search engines. A t 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 three (3) times in a row the account will be locked, the user ID disabled, and the user is locked out of the system until it can it is reset by the HMIS System Administrator. Passwords are always encrypted and can never be seen in clear text.

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, 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. 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 Record
In the ServicePoint HMIS, by default, all client project entry and exits are "Closed" except for the data elements used to aid in the de-duplication process. Those data elements are: name, social security number, date of birth, and veteran status. These data elements which consist of a

subset of Universal Data Elements (UDE's) are shared globally throughout the system so that each client has only one record in HMIS. 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 Record

If the client provides consent by signing a ROI form indicating their willingness to share information, users from other agencies would be able to see where the client is receiving services. Opening client information helps prevent the duplication of services to clients. All ROI's have a *start* and *end* dates. Data entered on or between the ROI's *start* and *end* date will be visible to other providers. Data entered before the *start* date or after the *end* date will not be visible to other providers because it is not covered by an ROI.

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 is ever reported outside of the system.

Provisions for Domestic Violence Providers

In October 2004, HUD issued a Clarification and Additional Guidance on Special Provisions for Domestic Violence Provider Shelters to supplement the HMIS Data and Technical Standards Final Notice. In this document, HUD exempts domestic violence providers from submission of client identifiers (name and SSN) to the CoC for deduplication and data analysis. Those programs electing that exemption are required to use either a proxy, coded, encrypted, or hashed unique identifier in lieu of name and SSN.

Summary

All parties – users, agencies, ADOH, the SYSTEM ADMINISTRATOR, Wellsky Corporation – take security & confidentiality very seriously. Violation of security & confidentiality is against the law. The AZBOSCOC has implemented extensive technical & procedural measures to protect client data.