HMIS SECURITY PLAN

The goal of the HMIS Security Plan is to ensure that HMIS data is collected, used, and maintained in a confidential and secure environment at all times. These standards represent a minimum level of security required for all HMIS participating agencies.

HMIS SOFTWARE PROVIDER

The Maricopa HMIS uses Wellsky's ServicePoint software. ServicePoint is supported by the very high system security including using 128-bit encryption, user authentication and user access levels. Wellsky' employees, who have access to client-level data, are subject to a national background check, training on confidentiality requirements, and must sign a confidentiality statement as part of their employee agreement. The system function logs the time and type of activity, as well as the name of the user who viewed, added, edited, or deleted the information.

Servers are located in complexes with:

- Twenty- four (24) hour security personnel.
- Twenty- four (24) hour video surveillance.
- Dedicated and secured Data Center.
- Locked down twenty- four (24) hours per day.
- Only accessible by management-controlled key.
- No access is permitted to cleaning staff.
- State-of-the-art HVAC and fire suppression system.

LEVELS OF USER ACCESS AND SECURITY

A licensed user is a person who has signed and submitted a Maricopa County HMIS Code of Ethics Agreement and completed basic user training. **Provider agencies are required to keep a copy of the HMIS Code of Ethics Agreement on file at the agency for all current users.** Provider agencies are required to immediately deactivate users and inform the HMIS System Administrator if a user leaves an agency within 24 hours of their termination or departure by submitting a ticket to the HMIS Help Desk. In addition, clients that do not actively use the system but retain a license pose a security risk. As a security measure, the HMIS team will audit the system once a month to determine which clients have not logged in for 45 days or more. Notification will be sent to these users and the point-of-contact at their agency that if they do not login within a week following the notice, their user account will be deactivated.

HMIS staff will provide each user a unique username and initial password. Users are not to share usernames, as this is a breach of the Maricopa County HMIS Code of Ethics agreement and the HMIS

Partnership Agreement. Exchanging usernames seriously compromises security and privacy of clients. If a breach occurs, it may subject the agency to discipline and termination of access to the Maricopa County HMIS system. HMIS conducts random audits of users to monitor that users are following the Maricopa HMIS Code of Ethics agreement.

HMIS Participating Agencies must establish an internal point of contact, known as the HMIS Primary Point of Contact, for establishing new users with the HMIS Administrator. Individual staff should not email or request new HMIS users or HMIS program changes without permission from the Agency Administrator. Agency Leadership should be copied on the correspondence so that they are aware of new user requests.

An agency must identify the type of user and programs each user should access within their agency.

SECURITY INCIDENT PROCEDURES

All HMIS Participating Agencies and their authorized users must abide by the terms of all HMIS agreements. Failure to fulfill these agreements may result in immediate termination of HMIS access until issues are resolved. All breaches related to security must be reported to the HMIS Lead Agency immediately after discovery. The HMIS Participating Agencies assumes all liability due to data breaches or risk of incident within their organization.

All HMIS users are obligated to report suspected instances of non-compliance with this policy that may leave HMIS vulnerable to intrusion or compromise client information. The HMIS Lead Agency and System Administrator is responsible for reporting any security incidents involving the real or potential intrusion.

All HMIS users will report any incident in which unauthorized use or disclosure of client information has occurred. Security breaches that have the possibility to impact the HMIS must be reported to the HMIS Participating Agency Administer who will notify the HMIS Lead Agency and System Administrator. Each HMIS Participating Agency will maintain and follow all procedures established by the HMIS Lead Agency, HMIS software and Maricopa County Regional Continuum of Care Board related to thresholds for security incident reporting.

If an unauthorized entity were to gain access to the Maricopa County HMIS and client data, or if there is suspicion of probable unauthorized access/activity, HMIS and Wellsky will take immediate action to protect the security of the system. HMIS will comply with all applicable laws and work with the affected Agencies to implement appropriate client notification.

AUDIT AND ACCESS CONTROLS

Wellsky maintains accessible audit trails that allows for the monitoring of user activity. They will also authenticate user activity via Internet Protocol address and present simultaneous user access.

All HMIS users are set up so that the HMIS uses the IP to validate the user. At no time and under no circumstance should an HMIS user share their user login and password or allow anyone to use their license. Each user is assigned their own unique user license.

PERSONAL AUTHENTICATION AND PASSWORD PROTOCOLS

All users are required to attend New User Training to obtain an HMIS license.

The below outlines password and user inactivity protocols for each HMIS User:

- All passwords must be unique
- All passwords must be rotated every 45 days
- All passwords must be in a prescribed format recommending a mix of letters/numbers/capitalization/symbols
- Upon the third unsuccessful login try, users will be locked out of the system. Users can select the "Forgot Password," option, request that their agency administrator reset their password or request that an HMIS administrator reset the password
- All users with no login activity for at least 45 days will be notified of inactivity. If after one week, there is no further feedback from the user, they will be automatically inactivated.

Agency Administrators may reset passwords. If the Agency Administrator is unavailable or otherwise unable to reset a password for an end user, HMIS will reset a user's password in the event the password is forgotten. Users must request a password reset by submitting a request to the Maricopa County HMIS Help Desk at www.hmisaz.org. Password resets will only be sent to the agency provided email address.

PUBLIC ACCESS PROTOCOLS

Program staff should be present to monitor workstations containing access to the HMIS database. Additionally, when workstations are not in use and staff is not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by the HMIS Participating Agency. If staff from an HMIS Participating Agency will be gone for an extended period of time, staff should log off the data entry system and shut down the computer. The HMIS database will automatically log the user out after 15 minutes of inactivity.

Users will ensure the confidentiality of client data, following all security policies in the Maricopa County HMIS Policies and Procedures Manual and adhering to the standards of ethical data use, regardless of the location of the connecting computer. The Agency Administrator or designee has the responsibility to assure the user is in compliance with this and all other policies, procedures, agreements and rules governing the Maricopa County HMIS.

All users that access the Maricopa County HMIS remotely must meet the standards detailed in this document and may only access it for activities directly related to their job. Users may not access the system from unsecured networks (for example: coffee shops, restaurants, libraries and other public places).

Examples of allowable Remote Access:
- Personal laptops that were not purchased by the agency.
- Access to the Maricopa County HMIS on a secured private network other than that of the agency.
- Private home desktops.

If a user is found to have accessed the Maricopa County HMIS through an unsecured network, the user license will be immediately suspended.

MALWARE AND VIRUS PROTECTION WITH AUTO UPDATE

HMIS Participating Agencies accessing the HMIS must protect the system by using commercially available malware, virus protection software, and must also maintain a secure firewall.

The HMIS Software Provider places firewalls on all data-hosting servers and regularly monitors all activity.

DISASTER PROTECTION AND RECOVERY

The HMIS Software Provider is contractually required to back up all HMIS data. Data backup is conducted every 24 hours and is maintained using both power and alternative power systems at a different location from the primary HMIS servers.

DATA SECURITY AND ENCRYPTION

Wellsky ensures availability of customer data in the event of a system failure or malicious access by creating and storing redundant records. All data going across the Internet to the user's Web browser uses AES-256 encryption in conjunction with RSA 2048-bit key lengths.

The traffic that flows between the server and the user's workstation is encrypted using the SSL certificate installed on CIR's dedicated servers. Database tape backups are performed nightly.

Tape backups are maintained in secure offsite storage. Seven (7) days' backup history is stored on instantly accessible Raid 10 storage. One (1) month's backup history is stored offsite. Users should report any experience of lag time or software down-time to the HMIS Help Desk by submitting a ticket. If system down-time occurs outside of the standard business hours, the users should contact the HMIS Manager or HMIS Director directly.