KC Metro HMIS
Homelessness Management Information System

SECURITY AND PRIVACY POLICY – HMIS LEAD AGENCY

The Mid-America Regional Council (MARC) serves as the Homelessness Management Information System (HMIS) Lead Agency for two Continuum of Care organizations (KS-505 and MO-604). The CaseWorthy HMIS system will serve over 50 agencies in the greater Kansas City area. MARC's privacy and security policy is designed to:

- Ensure the confidentiality, integrity, and availability of all HMIS information to protect clients served by local agencies
- Protect against any reasonable anticipated threats to security
- Ensure compliance by End Users to HUD and other federal, state and local rules

Key terms used

Covered Homeless Organization (CHO) – any organization (employees, volunteers, and contractors) that records, uses or processes Protected Personal Information

Protected Personal Information (PPI) – any information about a homeless client that (1) identifies a specific individual, (2) can be manipulated so that identification is possible, or (3) can be linked with other available information to identify a specific individual

Security Policy

MARC as the HMIS Lead Agency and each CHO must apply system security provisions to all systems where PPI is stored, including, but not limited to, the HMIS Lead Agency and CHO networks, desktops, laptops, tablets and servers. Security has three categories: system security, software application security, and hard copy security.

The following section (a) covers security for client data to be obtained for purpose of transitioning the data from the current HMIS vendor system, MAACLink, to the new system, CaseWorthy.

a. **System Security**

User Authentication: MARC as the HMIS Lead Agency will utilize CaseWorthy LLC's CaseWorthy system, an HMIS-compliant system with appropriate system level security. As MARC works to transition the CHOs from the current HMIS vendor to CaseWorthy, MARC will receive and evaluate HMIS client data for mapping data fields from one system to another and to identify duplicate records. MARC will receive the client records using a secure FTP site, and will store the records on a separate server that is password protected. The separate server will have SQL server 2016 with no Windows authentication and create SQL server accounts with specific permissions to access the database. MARC's two database analysts, the IT director and Network Administrator will have access to the server. MARC will also use SQL audits for tracking purposes. MARC will set up required password protection standards for use of this server. Once MARC has successfully completed mapping the current client data to CaseWorthy and no longer needs this server to complete the transition, the server will be cleaned of all data using procedures outlined below.

MARC as the HMIS Lead Agency will require a user authentication system consisting of a username and password. Passwords must be at least 8 characters long and meet reasonable industry standards, including but not limited to:

- At least one number and one letter
- Not using, or including, the username, the HMIS name, or the HMIS vendor's name, and/or
- Not consisting entirely of any work found in the common dictionary or any of the above spelled backwards

MARC s the HMIS Lead Agency will require users to change their passwords every 90 days. Users will be locked out from the system after 4 unsuccessful log in attempts. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users may not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Once the CaseWorthy system goes live, HMIS Lead Agency staff and CHO system users must follow the User Authentication requirements stated above.

Virus Protection: MARC as the HMIS Lead Agency and a CHO must protect the HMIS system from viruses by using commercially available virus protection software. The virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed, and regularly update virus definitions from the software vendor.

Firewalls: MARC as the HMIS Lead Agency and a CHO must protect the HMIS system from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the internet and other computer networks located outside the organization.

Public Access: NA. MARC may choose to implement a public portal to allow CHOs to have clients enter or update some of their information. At the time such a public portal is implemented, the CHO must follow HUD requirements for security protections.

Physical Access to Systems with Access to HMIS Data: A CHO must staff computers stationed in public areas that are used to access the CaseWorthy system at all times. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. MARC has established a timeframe of 60 minutes to log a user out of the system if not in active use. This log out will automatically show a password protected screen saver. A CHO may commit itself to additional security protections consistent with HMIS requirements, including timeframe to log users out of the system after a period of inactivity. MARC will require that all CaseWorthy system uses change their passwords every 90 days and only allow users to attempt unsuccessfully to log in four times before they are locked out of the system. A CHO may set more stringent standards for their users regarding changes to passwords or log in attempts.

Disaster Protection and Recovery: The CaseWorthy system operated by CaseWorthy LLC will maintain a backup to the system stored in a secure off-site location where the required privacy and security standards also apply. For purposes of working with client data during the transition from MAACLink to CaseWorthy, MARC as the Lead Agency will use a server, mini-computer or mainframe housed in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors must be used to protect systems used for collecting ad storing all of the HMIS data. If a CHO exports data from the CaseWorthy system and stores it electronically, the CHO will follow the same security measures as the HMIS Lead Agency described in this paragraph.

Disposal: In order to delete all HMIS data from a data storage medium, MARC and a CHO must reformat the storage medium more than once before reusing or disposing of the medium. When MARC disposes of servers, the agency wipes and/or destroys the drives. MARC wipes workstation drives before disposing.

System Monitoring: HMIS data must maintain a user access log. A CHO must use appropriate methods to monitor the security systems. CaseWorthy software includes a user history for all client records added, deleted, or modified.

b. **Software Application Security:** The CaseWorthy system meets all HUD requirements for Software Security during data entry, storage and review or other processing function. See User Authentication described above.

Electronic Data Transmission: MARC and a CHO must encrypt all HMIS data that are electronically transmitted over the Internet, publicly accessible networks or phone lines to current industry standards. The current standard is 128-bit encryption. Unencrypted data may be transmitted over section direct connections between two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data. A secure network would have secure direct connections.

Electronic Data Storage: MARC and a CHO must store all HMIS data in a binary, not text, format (CaseWorthy does this).

c. **Hard Copy Security:** MARC and a CHO must secure any paper or other hard copy containing PPI that is either generated by or for HMIS, including but not limited to reports, data entry forms and signed consent forms. MARC and a CHO must supervise at all times any paper or other hard copy generated by or for a HMIS that contains PPI when the hard copy is in a public area. The information must be secured when staff are not present.

HMIS Security Officer
As the HMIS Lead Agency, MARC must designate one staff member as the HMIS Security Officer. [MARC designates Helen Krosky, HMIS Project Manager, as the HMIS Security Officer.] If the designated employee changes, MARC will notify the two CoCs within 72 hours of the appointment of a new HMIS Security Officer.

Each agency using the system (CHO) must also designate a HMIS Security Officer to be responsible for ensuring compliance applicable security standards within their organization. The CHO Security Officer does not need to be an End User but they must be an employee of the participating organization. For any CHO without employees, the HMIS Security Officer must be the President, Chair, or other top-level representative responsible for the participating organization.

Workforce Security
The HMIS Lead Agency and each CHO must have a workforce security policy that includes conducting a criminal background check on its HMIS Security Officer and on any users with Agency Administrator level access or greater. Criminal Background checks must be completed at least once. On request, CHOs must verify to HMIS when the most recent criminal background check has been completed for each applicable staff member. The background check must include local and state records; CHOs are strongly encouraged to include federal records as well, but are not required.

Security and Privacy Awareness Training and Follow-up
The HMIS Lead Agency will conduct a security and privacy awareness training on an annual basis, which will be required for all End Users and Security Officers. This training will cover relevant statutory and regulatory requirements, local policies, and best practices for HMIS Privacy and Security. If an End User or Security Officer does not attend the required annual training, their access to CaseWorthy will be restricted until they attend training.

Reporting Security Incidents
Any End User or Security Officer suspecting violations of Security and Privacy policies should report incidents in writing.

Chain of Reporting: End Users should report issues first to their CHO's designated Security Officer within one business day. Security Officers should report the issue jointly to the CHO Director and the HMIS Lead Staff within one business day.

Disaster Recovery Plan

The Disaster Recovery Plan for HMIS is the responsibility of our HMIS Vendor, CaseWorthy, which hosts and houses the data on remote servers. The vender, CaseWorthy will perform regular scheduled backups of the system to prevent loss of data. In the event of a disaster involving substantial loss of data or system downtime, HMIS Lead Agency will contact CHO Security Officers by phone or email within one business day to inform them of the expected scale and duration of the loss or downtime.

Annual Security Review

All CHOs must undergo an annual security review, which will include at minimum the completion of a Security Checklist. Agency Administrators will work with the CHO Security Officer to schedule an audit and will assist with performing the review. The results of the annual review must be returned to the HMIS Security Officer via Fax or Email the same day they are completed. Any items needing to be fixed must be fixed within 10 working days.

Contracts and other arrangements

The HMIS Lead Agency must retain copies of all contracts and agreements executed as part of the administration and management of HMIS or required to comply with HUD policies.

PRIVACY POLICY

Data Collection Limitations: A CHO may collect PPI only after obtaining oral or written consent from the individual and using lawful and fair means. The CHO should only collect information when appropriate to the purpose for which it is obtained or when required by law. A CHO must post a sign at each intake desk (or comparable location) that explains the reasons for collecting the information.

Data Purpose and Limitations: A CHO must develop and implement a plan to dispose of or alternatively remove identifiers from PPI that is not in use for 7 years after the PPI was created or last changed (unless a statutory, regulatory, contractual or other requirement mandates longer retention). A CHO must specify in its privacy notice the purpose for which it collects PPI, including disclosure for the specified purpose. PPI may not be disclosed directly or indirectly for any government agency for inclusion in any national homeless database unless required by statute. The CHO must maintain an audit trail containing the date, purposes and recipient of some or all disclosures of PPI. The CHO must make the audit trail of disclosures available to the homeless individual on request.

Openness: A CHO must publish a privacy notice describing its policies and practices for the processing of PPI and provide a copy of the privacy notice to any individual upon request. A CHO must post a sign stating the availability of its privacy notice. The privacy notice may be amended at any time and that amendments may affect information obtained by the CHO before the date of the notice change. The CHO must make reasonable efforts to offer a client a copy of the privacy notice at or around the time of data collection.

Access and Correction: A CHO must allow an individual receiving services to inspect and have a copy of any PPI about the individual. There are circumstances when a CHO may reserve the ability to deny requests: anticipation of litigation, information obtained under a promise of confidentiality, or disclosure could endanger the life or physical safety of an individual. A CHO must offer to explain any information that the individual may not understand and consider any request by an individual for correction of inaccurate or incomplete PPI. A CHO is not required to remove any information, but may alternatively mark information as inaccurate or incomplete and supplement it with additional information.

Accountability: A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. The HMIS Lead Agency must offer annual training on privacy requirements, and a CHO must require each member of its staff to undergo the annual training. A CHO must require each member of its staff to sign a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

August 2017