Memphis and Shelby County Homeless Management Information System
Community Alliance for the Homeless, MIS Department
Memphis TN 38103
(901) 527-1302 Phone, (901) 527-1308 Fax
www.cafth.org

HMIS Privacy/Security Plan

MSCCOC HMIS PROJECT
PRIVACY PLAN

PURPOSE

This document describes the privacy plan of the Memphis/Shelby County Continuum of Care Homeless Management Information System (MSCCOC-HMIS) and agencies contributing data (HMIS Partnering Agencies) to the MSCCOC-HMIS. This document covers the processing of protected personal information for clients of HMIS Partnering Agencies.

Protected Personal Information is any information we maintain about a client that:

a. Allows identification of a client/consumer directly or indirectly
b. Can be manipulated by a reasonably foreseeable method to identify a specific client/consumer, or
c. Can be linked with other available information to identify a specific client/consumer.

The provisions of this plan shall go into effect immediately.

DATA COLLECTION NOTICE

HMIS Partnering Agencies must let clients know that personal identifying information is being collected, and the reasons for collecting this information. To meet this requirement, HMIS Partnering agencies must post the following language in places where intake takes place:

> Agency Name and its partner provider agencies collect personal information directly from you for reasons that are discussed in our NOTICE OF PRIVACY PRACTICES. Agency Name and its partner provider agencies may be required to collect some personal information by law or by organizations that provide funds to operate this project. Other personal information that is collected is important to run our projects, to improve services, and to better understand the needs of individuals being housed/sheltered/served. Agency Name and its partner provider agencies only collect information that is considered to be appropriate.

While the posted notice is the minimum requirement, agencies may choose to take additional steps to obtain consent from clients, including obtaining written consent. Agencies without a contractual relationship with Agency Name may use an Agency-specific alternative that complies with HUD's baseline privacy standards.

Each Agency should adopt and comply with the attached Notice of Privacy Practices for Use with the MSCCOC-HMIS ("HMIS Privacy Notice"). Agencies without a contractual relationship with Agency Name may use an Agency-specific alternative that complies with HUD's baseline privacy standards.

Each Agency must provide a copy of the *HMIS Privacy Notice* upon client request. Clients must acknowledge receipt by signing an *HMIS Client Consent Form.* Agencies without a contractual relationship with Agency Name may use an Agency-specific alternative. The Agency must keep signed copies of the *HMIS Client Consent Form.*

MSCCOC HMIS PROJECT
PRIVACY PLAN

Each Agency shall provide reasonable accommodations to persons with disabilities and to persons with limited English proficiency to ensure their understanding of the HMIS Privacy Notice and/or Acknowledgement Form.

ACCOUNTABILITY

Each agency must uphold relevant federal and state confidentiality regulations and laws that protect client records, including but not limited to the privacy and security standards found in HUD's Data and Technical Standards. If the Agency is a HIPAA-covered entity, the Agency is required to operate in accordance with HIPAA regulations and is exempt from the privacy and security standards found in HUD's Data and Technical Standards.

ACCESS AND CORRECTION

Each agency must allow individuals to inspect and have a copy of their personal information that is maintained in HMIS.

Each agency must offer to explain any information that is not understood.

Individuals must submit a request to inspect their HMIS data in writing to their social worker/case manager. Each agency must consider a written request for correction of inaccurate or incomplete personal information. If the agency agrees that the information is inaccurate or incomplete, the agency may delete it or may choose to mark it as inaccurate or incomplete and to supplement it with additional information.

Each agency may deny the individual's request for inspection or copying of personal information if:

a. Information was compiled in reasonable anticipation of litigation or comparable proceedings
b. Information is about another client/consumer
c. Information was obtained under a promise of confidentiality and the disclosure would reveal the source of the information, or
d. Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If the agency denies a request for access or correction, it must explain the reason for the denial and include documentation of the request and the reason for the denial.

Each agency may reject repeated or harassing requests for access or correction.

PURPOSE AND USE LIMITATIONS

Each agency will use or disclose personal information for activities described in this part of the notice. The agency assumes that clients consent to the use or disclosure of personal information for the purposes described here and for other uses and disclosures that are determined to be compatible with these uses or disclosures:

MSCCOC HMIS PROJECT
PRIVACY PLAN

a. To provide or coordinate services to individuals (shelter, housing, case management, etc.)
b. For functions related to payment or reimbursement for services
c. To carry out administrative functions such as personnel oversight, management functions, and auditing purposes.
d. To create de-identified (anonymous) information that can be used for research and statistical purposes
e. When required by law
f. To avert a serious threat to health or safety if:
    i. the agency believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
    ii. the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat
g. To report victims of abuse when authorized by law.
h. For research purposes unless restricted by other federal and state laws.
i. To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct).
j. For judicial and administrative proceedings in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena.
k. To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

Before any use or disclosure of personal information that is not described here, the agency must seek the clients consent first.

CONFIDENTIALITY

Each agency must maintain any/all personal information as required by federal, state, or local laws.

Each agency shall only solicit or input into HMIS client information that is essential to providing services to the client.

Each agency shall not knowingly enter false or misleading data under any circumstance, nor use HMIS with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.

Each agency shall ensure that all staff, volunteers and other persons who use HMIS are issued an individual User ID and password.

Each agency shall ensure that all staff, volunteers and other persons issued a User ID and password for HMIS receive confidentiality training, HMIS training, and comply with the attached *HMIS User Agreement* and the *HMIS Participation Agreement*.

MSCCOC HMIS PROJECT
PRIVACY PLAN

PROTECTIONS FOR VICTIMS OF DOMESTIC VIOLENCE, DATING VIOLENCE, SEXUAL ASSAULTS AND STALKING

Victim service providers are prohibited from entering data into HMIS. Other agencies must be particularly aware of the need for confidentiality regarding information about persons who are victims of domestic violence, dating violence, sexual assault, and stalking. Additional protections for these clients includes explicit training for staff handling personal identifying information of the potentially dangerous circumstances that may be created by improper release of this information.

MSCCOC HMIS PROJECT
SECURITY PLAN

This plan describes the standards for the security of all data contained in the Memphis/Shelby County Continuum of Care Homeless Management Information System (MSCCOC-HMIS). This plan outlines the security measures currently implemented by the HMIS Lead Agency, the Community Alliance for the Homeless (CAFTH) and details the baseline security requirements for all HMIS Partnering Agencies.

Applicability

CAFTH, MIS Department and HMIS Partnering Agencies must apply system security provisions to all the systems where personal protected information (PPI) is stored, including, but not limited to, its networks, desktops, laptops, mini-computers, mainframes and servers.

User Authentication

Upon successful completion of training and subject to approval by CAFTH, MIS Department Staff, each HMIS user will be provided with a unique personal User Identification Code (User ID) and initial password to access the HMIS.

While the User ID provided will not change, HUD standards require that the initial password only be valid for the user's first access to the HMIS. Upon access with the initial password, the user will see a screen that will prompt the user to change the initial password to a personal password created by the user.

1. Only the user will know the personal password he or she creates. It is the user's responsibility to remember the password.

2. The password created by the user must be meet the following Federal and application-enforced guidelines:
    - The password must be at least eight characters long.
    - The password must contain at least one letter.
    - The first character of the password must be a letter.
    - The password must contain at least one number.
    - The password must contain at least one symbol or punctuation character.
    - The password may not contain your User ID.
    - The password may not contain the consecutive upper- or lower-case letters “HMIS” or “hmis.”

    Providers are responsible for communicating all staff departures to the CAFTH, MIS Department Manager in a timely manner to ensure user profiles for departed staff are inactivated.

3. The password may not be stored in a publicly accessible location and written information pertaining to the User ID, password, or how to access the HMIS may not be displayed in any publicly accessible location.

4. The user is not permitted to divulge this password or to share this password with anyone.

MSCCOC HMIS PROJECT
SECURITY PLAN

Before logging in to the HMIS, the user must check a box agreeing to the HMIS User Agreement which was established by Bowman System in cooperation with the Memphis/Shelby County Continuum of Care.

Application Security

HMIS Partnering Agencies must maintain anti-virus software on all PC's on their network. PC's that access the Internet must be configured to automatically download updated virus definitions. Steps should also be taken to prevent the intrusion of "adware" and "spyware" programs.

Agency Name maintains hardware, software and PPI in a secure environment, protected by a Firewall.

Public Access

End users connect to the MSCCOC-HMIS through the public Internet via a Secure Socket Layer (SSL) Public Key Infrastructure (PKI) tunnel connection.

Physical Access to HMIS Data

HMIS Partnering Agencies must staff computers at all times that are stationed in public areas and used to collect and HMIS data. Every computer that is used to access the HMIS must have a password-protected screen saver that automatically turns on when the computer is temporarily not in use. If an HMIS user will be away from the computer for an extended period of time, he or she is required to log off from HMIS before leaving the work area in which the computer is located.

Disaster Protection and Recovery

HMIS data is contained on SQL 2005 databases which are run on a Windows Server clustered environment so that there will failover if the primary server becomes unavailable. The physical data storage is on multiple disc drives in a RAID array for redundancy so that no data will be lost or downtime incurred if a physical disk drive becomes inoperable. Additional hardware redundancy exists in the form of dual power supplies, disc controllers and network interface cards. CAFTH maintains service coverage through original and extended warranties from the original equipment manufacturer and assures that the systems are kept up to date in terms of patches and updates issued by both the software and hardware vendors. The SQL databases are automatically backed up nightly and stored on another secure server. The HMIS database server itself is located in a controlled, physically secured environment at bowman Systems in Shreveport LA and is protected by modern systems for HVAC and Fire Suppression which are monitored 24/7. A diesel generator is maintained for backup power, and redundant Internet connections exist on opposite sides of the building. The Terminal Servers are in a office location where they are also behind a locked door in a building that has 24/7 security.

Disposal

The Community Alliance for the Homeless contracts with a certified specialist for destruction of physical disk drives who can be utilized as required.

System Monitoring

HMIS produces reports based on log files that are reviewed and inactive user accounts are consequently disabled. In addition to the HMIS database itself, access to HMIS is also controlled, monitored and logged by the Active Directory (AD) and Checkpoint security systems.

MSCCOC HMIS PROJECT
SECURITY PLAN

Electronic Data Storage

HMIS data is contained on SQL 2005 databases which are run on a Windows Server clustered environment; and therefore, is stored in binary format.

Hard Copy Security

The guidelines regarding the security of paper or other hard copy containing PPI that is either generated by or for the HMIS, including, but not limited to reports, data entry forms, and signed consent forms are:

1. HMIS Partnering Agency staff must supervise at all times any paper or other hard copy generated by or for the HMIS that contains PPI when the hard copy is in a public area.
2. When HMIS Partnering Agency staff is not present, the information must be secured in areas that are not publicly accessible.
3. Written information specifically pertaining to user access (e.g., User ID and password) must not be stored or displayed in any publicly accessible location.

Duration

This plan must be reviewed annually and updated as needed by the MSCCOC MIS Committee.