Knoxville Homeless Management Information System
(865) 974-9142
hmissupport@utk.edu
www.KnoxHMIS.org

KnoxHMIS Privacy Plan

KnoxHMIS
Privacy Plan

Purpose

This document describes the privacy plan of the Knoxville-Knox County Homeless Management Information System (KnoxHMIS) and agencies contributing data (HMIS Partnering Agencies) to the KnoxHMIS. 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 KnoxHMIS ("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 Notices of Uses and Disclosures* upon client request. Clients must acknowledge receipt by signing an *HMIS Notice to Clients of Uses and Disclosures*. Agencies without a contractual relationship with Agency Name may use an Agency-specific alternative. The Agency must keep signed copies of the *HMIS Notice to Client of Uses and Disclosures.*

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:

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*.

In case of a breach, an agency shall contact the Lead HMIS within 30 (thirty) calendar days after the discovery of the breach.

In the case that a client requests that a HMIS Member Agency rescind the disclosure of protected health information, the HMIS Member agency must comply except:

- as otherwise required by law, the disclosure is to a health plan for carrying out payment or health care options, and
- the protected health information pertains to a health care item or serve for which the provider involved has been paid out of pocket in full.

In no situations should a HMIS Member Agency, directly or indirectly, receive remuneration in exchange for any protected health information of a client.

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.