KnoxHMIS Privacy Notice

Purpose

KnoxHMIS is the Homeless Management Information System (HMIS) for Knoxville and Knox County, Tennessee. This document ("Privacy Notice") describes the privacy protections set in place by KnoxHMIS and its Partner Agencies ("Agencies") entering data into HMIS. This Privacy Notice covers how KnoxHMIS handles **Personally Identifiable Information (PII)** for the Agencies' Clients. PII is any information that is specific enough to identify a person, either on its own or combined with other data.

Partner Agency Responsibilities

Agencies are required to adopt and comply with all the privacy protections detailed in this Privacy Notice. Agencies are encouraged to provide a copy of this Privacy Notice to each Client, and must:

- Inform Clients that PII is being collected and provide the reasons for collecting this information.
- Post this Privacy Notice visibly in places where intakes occur.
- Provide a copy of this Privacy Notice, the KnoxHMIS Release of Information, and KnoxHMIS Partner Poster (listing all agencies with HMIS access) upon Client request.

While posting this Privacy Notice is the minimum requirement, Agencies may choose to take additional steps to ensure the Client is fully informed, e.g., by guiding the Client through this Privacy Notice and answering questions as needed. Agencies shall provide reasonable accommodations to persons with disabilities and persons with limited English proficiency to ensure their understanding of the KnoxHMIS Privacy Notice and the KnoxHMIS Release of Information Form (ROI).

Accountability

Agencies 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 an 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

Agencies must allow Clients to view their personal information recorded in HMIS and provide Clients a copy upon their request. Clients have a right to rescind their consent for HMIS partners to share Client information; data already entered will not be un-shared, but data for projects entered thereafter will be locked down.

Agencies must offer to explain any information that is not understood.

Clients must request to view their HMIS data in writing to their social worker/case manager. Agencies 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.

Agencies may deny the Client'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 person
c. Information was obtained under a promise of confidentiality and 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 person.

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.

Agencies may reject repeated or harassing requests for access or correction.

Purpose and Use Limitations

Agencies may use or disclose personal information for purposes 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 internally manage data related to programs and services such as shelter, case management, and the provision of basic needs.
b. To complete functions related to payment or reimbursement for services,
c. To carry out administrative functions such as staff oversight management functions, and auditing purposes;
d. To create de-identified (anonymous) information that can be used for research and statistical purposes or for reporting to funders, the general public, or key decision makers for the purposes of informing future homeless services efforts. *(No names, date of birth, or other personally identifiable information beyond numeric Client ID will be shared.)*;
e. To avert a serious threat to health or safety if:
    the agency believes that the use or disclosure is necessary to prevent or lessen (1) a public health crisis or (2) a serious and imminent threat to the health or safety of a Client or the public, and the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat;
f. To report victims of abuse when required by law;
g. To deduplicate Client records (i.e. share just enough information to ensure that each Client is only entered into HMIS once, e.g., by sharing name, age, and social security number within the secure HMIS platform);
h. To coordinate care between street outreach teams when Client is staying in places not meant for habitation

i. 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, again only as required by law;
j. For oversight of compliance with HMIS requirements.

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

Confidentiality

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

Agencies may only access or enter Client information when it is necessary for providing services to the Client.

Under no circumstances may Agencies knowingly enter false or misleading data, or use HMIS with intent to defraud federal, state or local governments, Clients or entities, or to conduct any illegal activity.

Agencies shall ensure that all HMIS users are trained through HMIS and comply with the *KnoxHMIS User License & Policy Agreement*.

HMIS users are not permitted at any time to share their HMIS username and password with anyone else, including fellow staff members or volunteers.

If an Agency discovers data was shared beyond the scope of this Privacy Notice, they shall contact KnoxHMIS within 7 (seven) calendar days.

In no situations should an 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 supported by Violence Against Women Act (VAWA) funding are prohibited from entering data into HMIS. 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 regarding the potentially dangerous circumstances that may be created by improper release of Victims' personally identifiable information.

The provisions of this Privacy Notice shall go into effect immediately. This Privacy Notice may be revised at any time, and amendments may affect data entered before such changes were made.

For more information, please contact KnoxHMIS support staff at (865) 974-9217 or HMISsupport@utk.edu.