AKHMIS

Confidentiality and Ethics Review

What are the confidentiality requirements?

- For all information entered in the HMIS system, Service Providers, Users, and Agencies are bound by all applicable federal and state confidentiality regulations and laws that protect Client records that will be accessed or entered into the HMIS system.
- HIPAA Privacy Rules take precedence over HMIS privacy standards. If an agency is a HIPAA covered agency, they must abide by HIPAA regulations.

Confidentiality

- Some of the data HMIS collects is considered Protected Personal Information (PPI). Protected Personal Information is defined as: Any information that can be used to identify a particular individual.

- Protected Personal Information includes without limitation a Clients name, Social Security Number, Date of Birth, and such personal identifying information that identifies directly, indirectly, by linking with other identifying information to identify a specific individual, or can be manipulated by a reasonably foreseeable method to identify an individual.

- Any requests for release of information, including court orders and subpoenas, shall be referred to the Administrator.
- Users and Agencies agree not to release any confidential information received from the HMIS database to any organization or individual.

HMIS Use and Responsibilities

- It is everyone's responsibility; in all agency/programs, Users, and the HMIS System Administrator.

- Agencies/Programs will comply with all policies and procedures of HMIS and shall keep abreast of all ServicePoint updates and policy changes.

Agency/Program Responsibilities

- The agency/program who receives HUD funding (SHP, ESG, S+C, etc) participating in HMIS must be current in all related contracts.

- A/P will identify, approve and authorize their respective Users and is responsible for contacting the HMIS System Administrator for revoking, adding or editing User access.

- A/P and their authorized Users shall not misrepresent their client base in the HMIS database by entering known, inaccurate, false or misleading data under any circumstances.

- A/P will not alter information, with known inaccurate information, that has been entered into the HMIS database by another Service Provider, Agency, or User.

- A/P and their authorized Users shall not cause in any manner or way known corruption of the HMIS database.

- A/P will report any discrepancies in the use of the HMIS system, including without limitation access of information and entry of information, to the Agency Director or to the HMIS System Administrator.

- *The use of the HMIS database with the intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity, will be grounds for legal action.*

- A/P shall utilize the HMIS Client Consent & Release of Information Authorization form for all Clients.
- A/P shall provide a verbal explanation of the HMIS database and the terms of consent to the Client, including an explanation of how the information will be used, how it will be provided, and advantages of providing accurate information.

- A/P shall maintain appropriate documentation of Client consent to participate in the HMIS database.

- A/P shall diligently record and take appropriate actions, in the HMIS system, to record all restrictions requested by the Client.

- If a Client withdraws consent for release of information, A/P remains responsible to ensure that Clients information is restricted.

- A/P must publish a privacy notice describing its policies and practices for the processing of PPI (Personal Protected Information) and must provide a copy of its privacy notice to any individual upon request.

- A/P must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures

- A/P must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information.

- A/P must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

- A/P shall be responsible for entering Client data (profile, household, needs, services, referrals, any other Client data you may require), following up on referrals, running reports.

- A/P shall provide an email contact to the System Administrator for each User for communication purposes.

- A/P shall have representation at all agency/regional data quality review meetings.
- A/P shall be responsible for HMIS data entry compliance for client data and reports.
- A/P are responsible for the Users data entry accuracy, correctness and completeness. They shall periodically (or when requested by the System Administrator) run and review audit reports to ensure data integrity.

- A/P shall follow, comply with and enforce the User Agreement. (The User Agreement may be modified, with notification, AKHMIS at its discretion, as needed for the purpose of efficient operation of the HMIS system).

A/P shall be responsible for entering into HMIS:

- HUD funded Agency/Programs– Universal Data Elements (client profile, household, entry/exit, services, and shelter), and any Program Specific data as required by the grant. (High lighted in red in Service Point)

- Non-HUD funded Agency/Programs– at a minimum the Universal Data Elements (client profile, household, entry/exit, services, and shelter).

User Code of Ethics

A. Users must be prepared to answer Client questions regarding AKHMIS.

B. Users must faithfully respect client preferences with regard to the entry and sharing of client information within AKHMIS. Users must accurately record client's preferences by making the proper designations as to sharing of client information and/or any restrictions on the sharing of client information.

C. Users must allow Client to change his or her information sharing preferences at the Client's request.

D. Users must not decline services to a Client or potential Client if that person refuses to share their personal information with other service providers via AKHMIS.

E. User has primary responsibility for entering truthful, accurate and complete information.

F. Users will not solicit from or enter information about Client into AKHMIS unless the information is for a legitimate business purpose, such as to provide services to the Client.

G. Users will not alter or override information entered by a Partner Agency.

H. Users will not include profanity or offensive language in AKHMIS; nor will Users use AKHMIS database for violation of any law, to defraud any entity or conduct illegal activity.

I. Upon Client request Users must allow Client to inspect and obtain a copy of the Client's own information maintained within AKHMIS. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding need not be provided to Client.

J. Users must permit Clients to file a written complaint regarding the use or treatment of their information within AKHMIS. Client may file a written complaint with the Agency or the Municipality of Anchorage, AKHMIS (c/o MOA, Department of Health and Human Services, Safety Links Program, LINK Project, P.O. Box 196650, Anchorage, Alaska 99519-6650). Clients may not be retaliated against for filing a complaint.

Any Questions????

Please remember…

- Should you have any questions, please contact *John* (343-6593) burgerjj@muni.org, *Sandy*(343-6592) olibricesm@muni.org or *Melissa*(343-6535) andersonmt@muni.org
- Or our joint support email address:

akhmissupport@muni.org.

Thank you for listening!

Cheers!