Alaska Homeless Management Information System (AKHMIS)
Privacy Policy

Use and Disclosure of Personal Information

These policies explain why an Agency collects personal information from clients. Personal information may be used or disclosed for activities described in this part of the notice. Client consent to the use or disclosure of personal information for the purposes described in this notice, and for reasons that are compatible with purposes described in this notice but not listed, is assumed. Clients must give consent before their personal information is used or disclosed for any purpose not described here.

Personal information may be used or disclosed for the following purposes:

1. *To provide or coordinate services to individuals. Services may include but are not limited to, X, Y, Z.*
2. Sharing of data input and generated by AKHMIS shall be limited outside of the system to the greatest extent possible. If there is a need to share or reference an AKHMIS file, only the client file number may be shared via email.

3. To carry out administrative functions such as legal audits, personnel, oversight, and management functions.

4. To inform the community, de-identified aggregate data reports are available upon request.

5. With client consent, identifiable information can be shared with third parties to improve service delivery.

6. For academic research conducted by an individual or institution that has a formal relationship with the respective Continuum of Care. The research must be conducted by an individual employed by or affiliated with the organization or institution. All research projects must be conducted under a written research agreement approved in writing by the Continuum of Care's Executive Committee. The written research agreement must:
    - Establish the rules and limitations for processing personal information, and provide security for personal information in the course of the research;
    - Provide for the return or proper disposal of all personal information at the conclusion of the research;
    - Restrict additional use or disclosure of personal information, except where required by law;
    - Require that the recipient of the personal information formally agree to comply with all terms and conditions of the written research agreement; and
    - Be substituted, when appropriate, by Institutional Review Board, Privacy Board, or other applicable human subjects' protection institution approval.

7. When required by law, personal information will be released to the extent that use or disclosure complies with the requirements of the law.

8. To avert a serious threat to health or safety if:
    - 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
    - The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

9. To report to a governmental authority (including a social service or protective services Agency) authorized by law to receive reports of abuse, neglect or domestic violence, information about an individual reasonably believed to be a victim of abuse, neglect, or domestic violence. When the personal information of a victim of abuse, neglect, or domestic violence is disclosed, the individual whose information has been released will promptly be informed, except if:
    - It is believed that informing the individual would place the individual at risk of serious harm, or
    - A personal representative (such as a family member or friend) who is responsible for the abuse, neglect, or other injury is the individual who would be informed, and it is believed that informing the personal representative would not be in the best interest of the individual as determined in the exercise of professional judgment.

10. For a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

    - In response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer or a grand jury subpoena, if the court ordered disclosure goes through the Agency that received the legal document and is reviewed by the Executive Director for any additional action or comment.
    - If the law enforcement official makes a written request for personal information. The written request must meet the following requirements:
        i. Be signed by a supervisory official of the law enforcement Agency seeking the personal information;
        ii. State how the information is relevant and material to a legitimate law enforcement investigation;
        iii. Identify the personal information sought;
        iv. Be specific and limited in scope to the purpose for which the information is sought; and
        v. Be approved for release by the originating Agency's legal counsel after a review period of seven to fourteen days.
    - If it is believed that the personal information constitutes evidence of criminal conduct that occurred at the Agency where the client receives services.
    - If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to a foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

11. For law enforcement or another public official authorized to receive a client's personal information to conduct an immediate enforcement activity that depends upon the disclosure. Personal information may be disclosed when a client is incapacitated and unable to agree to the disclosure if waiting until the individual is able to agree to the disclosure would materially and adversely affect the enforcement activity. In this case, the disclosure will only be made if it is not intended to be used against the individual.

12. To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

Inspection and Correction of Personal Information

Clients may inspect and receive a copy of their personal information maintained in AKHMIS. The Agency where the client receives services will offer to explain any information that a client may not understand.

If the information listed in AKHMIS is believed to be inaccurate or incomplete, a client may submit a verbal or written request to have his / her information corrected. Inaccurate or incomplete data may be deleted or marked as inaccurate or incomplete and supplemented with additional information.

A request to inspect or copy one's personal information may be denied if:

- The information was compiled in reasonable anticipation of litigation or comparable proceedings;
- The information was obtained under a promise of confidentiality and if the disclosure would reveal the source of the information; or
- The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information.

If a request for inspection access or personal information correction is denied, the Agency where the client receives services will explain the reason for the denial. The client's request and the reason for the denial will be included in the client's record.

Requests for inspection access or personal information correction may be denied if they are made in a repeated and / or harassing manner.

Limits on Collection of Personal Information

Only personal information relevant for the purpose(s) for which it will be used will be collected. Personal information entered into AKHMIS must be as accurate and complete as possible. Clients cannot be denied services for refusal to provide personal information.

Client files not used in seven years may be made inactive in AKHMIS. ICA will check with agencies before making client files inactive. Personal information may be retained for a longer period if required by statute, regulation, contract, or another obligation.

Limits on Partner Agency Use of AKHMIS Client Information

The AKHMIS is a data system with limited sharing agreements in place. Providers have the option of defaulting client-level data to share with other providers in HMIS or changing individual client record settings to share some or all of a client's data, if the applicable data sharing agreements are in place. Youth providers serving clients under the age of 18 must maintain closed AKHMIS client files, unless the provider is able to obtain a Client Informed Consent and Release of Information from the youth's legal guardian. Youth under the age of 18 may not provide either written or verbal consent to the release of their personally identifying information in AKHMIS.

Complaints and Accountability

Questions or complaints about the AKHMIS privacy and security policies and practices shall be submitted to the Agency where the client receives services.

All AKHMIS users (including employees, volunteers, affiliates, contractors, and associates) are required to comply with this privacy notice. Users must receive and acknowledge receipt of a copy of this privacy notice.