Alaska Homeless Management Information System (AKHMIS)

AKHMIS Policies and Procedures

CONTENTS

1 INTRODUCTION

To provide more effective services to individuals across the State of Alaska who are at-risk of or experiencing homelessness, service providers have joined with the Institute for Community Alliances (ICA) to effectively implement the Alaska Homeless Management Information System (AKHMIS). Although the AKHMIS was initiated to meet the United States Department of Housing and Urban Development's (HUD) data collection requirements, the Alaska Continuums of Care (AK CoCs) and the HMIS Lead Agency (ICA) are working to make it an attractive tool for all covered homeless organizations (CHOs).

Funding for the AKHMIS comes from the HUD Continuum of Care (CoC) grants and match dollars from the Alaska Housing Finance Corporation (AHFC). ICA will provide technical assistance and training related to the AKHMIS. Aggregated, anonymous data from the AKHMIS will be used to generate reports for federal, state, and local funders.

AKHMIS data will be available to inform communities, stakeholders, and other interested parties regarding homelessness prevention and intervention services across the State of Alaska. The AK CoCs will use AKHMIS data to make data-informed decisions regarding homeless services, covered homeless organizations, and programs to ensure the effectiveness of the AK CoCs in providing services to reduce and end homelessness.

The AK CoCs have adopted the use of WellSky Community Services^{TM} as its platform for a statewide HMIS. WellSky Community Services^{TM} is a secure, web-based application that can be accessed through encrypted internet connections.

In addition to client-level data entered by CHOs, the AKHMIS is also used to record demographic data and produce reports for the annual Point-in-Time (PIT), Longitudinal System Analysis (LSA), Annual Performance Reports (APRs), System Performance Measures (SPMs), and other required reports provided annually, quarterly, or for any other time period requested by federal, state, or local funders.

Effective implementation of the AKHMIS will benefit individuals and families at-risk of or experiencing homelessness, covered homeless organizations, organization directors, public policy planners, and the community.

Guidance for the effective implementation of the AKHMIS is provided by the Executive Committees of the AK CoCs, with input from the statewide AKHMIS Advisory Board.

This document provides the policies, procedures, guidelines, and standards that govern AKHMIS operations, as well as the responsibilities for Covered Homeless Organization Program Directors and AKHMIS Users.

AKHMIS BENEFITS

Use of the AKHMIS provides numerous benefits for persons at-risk of or experiencing homelessness, CHOs, and the AK CoCs.

BENEFITS FOR PERSONS AT-RISK OF OR EXPERIENCING HOMELESSNESS:

- Intake information and needs assessments are maintained historically, reducing the number of times persons at-risk of, or experiencing homelessness must repeat their stories to multiple CHOs;
- The opportunity to provide intake and life history only once demonstrates that CHOs value the time of those at-risk of or experiencing homelessness, and restores some of the client's dignity; and,
- Multiple services can easily be coordinated, and referrals can be streamlined to ensure clients are matched appropriately to services to end their housing crisis as quickly as possible.

BENEFITS FOR CHOS AND THE AK COCS:

- Provides online, real-time information about client needs and the services available for persons at-risk of or experiencing homelessness;
- Ensures client confidentiality by providing information in a secured system;
- Decreases duplicative client intakes and assessments;

- Tracks client outcomes and provides a client history;
- Generates data reports for local use, and for state and federal reporting requirements;
- Facilitates the coordination of services within and among CHOs;
- Provides access to a statewide database of CHOs, allowing staff to easily select a referral organization;
- Assists in defining and understanding the extent of homelessness throughout the State of Alaska;
- Aids in focusing staff and financial resources where services for persons experiencing homelessness are needed the most;
- Works to evaluate the effectiveness of specific interventions and projects, as well as services provided; and
- Assists the community in utilizing data-informed solutions to reduce and end homelessness.

2 PRIVACY

This Policy describes standards for the privacy of personal information collected and stored in the Alaska Homeless Management Information System (AKHMIS), as well as personal information collected for the purposes of the Coordinated Entry Systems for the two Continuums of Care (AK CoCs) across the State of Alaska – Anchorage CoC and Balance of State CoC. The standards seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. This Privacy Policy (hereinafter referred to as "Policy") is based on principles of fair information practices recognized by the information privacy and technology communities.

This Policy defines the privacy standards that will be required of any organization within the State of Alaska that records, uses, or processes personally identifiable information (PII) on clients at-risk of or experiencing homelessness for the AKHMIS, and / or the CoCs Coordinated Entry System (CES) process. Organizations must also comply with federal, state, and local laws that require additional confidentiality protections, where applicable.

This Policy recognizes the broad diversity of organizations that participate in the AKHMIS and / or the CES processes, and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations (e.g., such as those serving victims of domestic violence) may choose to implement higher levels of privacy standards because of the nature of the clients they serve and / or service provision. Others (e.g., large emergency shelters) may find higher standards overly burdensome or impractical. At a minimum, however, all organizations must meet the privacy standards described in this Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for organizations with additional needs or capacities.

The following sections discuss the **Alaska Continuums of Care Statewide Privacy Policy (AK CoC Statewide Privacy Policy).**

2.1 ALASKA COC STATEWIDE PRIVACY POLICY (AK COC STATEWIDE PRIVACY POLICY)

DEFINITIONS

Personally Identifiable Information (PII): Any information maintained by or for a Covered Homeless Organization about a client at-risk of or experiencing homelessness that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Coordinated Entry System (CES): a process developed to ensure that all people experiencing a housing crisis have fair and equal access and are quickly identified, assessed for, referred, and connected to housing and assistance based on their strengths and needs

Covered Homeless Organization (CHO): Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, or processes PII on clients at-risk of or experiencing homelessness for an HMIS or CES. This definition includes both organizations that have direct access to the AKHMIS and/or the AK CoCs CES, as well as those organizations who do not have direct access to the AKHMIS but do record, use, or process PII.

Processing: Any operation or set of operations performed on PII, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission, and destruction of the information.

AKHMIS and CES Uses and Disclosures: The uses and disclosures of PII that are allowed by this Policy.

Uses and Disclosures: Uses are activities internal to a CHO that involves interaction with PII. Disclosures are activities in which a CHO shares PII externally.

SCOPE & APPLICABILITY

This Policy applies to any homeless assistance organization that records, uses, or processes personally identifiable information (PII) for the AKHMIS and / or an AK CoCs' CES. A provider that meets this definition is referred to as a Covered Homeless Organization (CHO).

HIPAA CONSIDERATIONS

All Partner Agencies are expected to uphold federal, state, and local confidentiality regulations to protect records and privacy. If an agency is covered by the Health Insurance Portability and Accountability Act (HIPPA), the HIPAA regulations prevail.

ALLOWABLE AKHMIS AND CES USES AND DISCLOSURES OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Client consent for any uses and disclosures defined in this section is assumed when organizations follow HUD HMIS Standards for notifying clients of privacy policies.

A CHO may use or disclose PII from the AKHMIS, and/or the CoCs' CES under the following circumstances:

- To provide or coordinate services for an individual or household;
- For functions related to payment or reimbursement for services;
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight, and management functions;
- When required by law;
- For research and/or evaluation; or
- For creating de-identified PII.

CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of clients. The following additional uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible and limited way. Under this Policy, these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with this Policy). However, nothing in this Policy modifies an obligation under applicable law to use or disclose personal information.

Uses and disclosures required by law. A CHO may use or disclose PII when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

Uses and disclosures to avert a serious threat to health or safety. A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:

- The CHO, in good faith, believes 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.

Uses and disclosures about victims of abuse, neglect, or domestic violence. A CHO may disclose PII about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services organization) authorized by law to receive reports of abuse, neglect or domestic violence under the following circumstances:

- Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
- If the individual agrees to the disclosure; or
- To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violencemust promptly inform the individual that a disclosure has been or will be made, except if:

- The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at-risk of serious harm; or
- The CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the CHO, in the exercise of professional judgment.

Uses and disclosures for academic research or evaluation purposes. A CHO may use or disclose PII for academic research or evaluation conducted by an individual or institution that has a formal relationship with the CHO, if the research/evaluation is conducted either:

- By an individual employed by or affiliated with the research/evaluation entity where the research/evaluation project is conducted under a written research/evaluation agreement approved in writing by a program administrator (other than the individual conducting the research/evaluation) designated by the CHO or
- By an institution for use in a research/evaluation project conducted under a written research/evaluation agreement approved in writing by a program administrator designated by theCHO.

A written research/evaluation agreement must:

- Establish rules and limitations for the processing and security of PII in the course of the research/evaluation;
- Provide for the return or proper disposal of all PII at the conclusion of the research/evaluation;
- Restrict additional use or disclosure of PII, except where required by law; and
- Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written research/evaluation agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board, or other applicable human subjects' protections.

Any research/evaluation on the nature and patterns of homelessness (at the CoC-wide or system-wide level) that uses PII AKHMIS data will take place within the bounds of specific agreements between researchers and the entity that administers the AKHMIS. These agreements must be approved by the Executive Committee(s) of the Board(s) of Director(s) for the applicable CoC(s) and must reflect adequate standards for the protection of confidentiality of data.

Disclosures for law enforcement purposes. A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII for a law enforcement purpose to a law enforcement official under any of the following 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 law enforcement official makes a written request for protected personal information that:
- Is signed by a supervisory official of the law enforcement organization seeking the PII;
- States that the information is relevant and material to a legitimate law enforcement investigation;
- Identifies the PII sought;
- Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
- States that de-identified information could not be used to accomplish the purpose of the disclosure.
- If the CHO believes in good faith that the PII constitutes evidence of criminal conduct that occurred on the premises of the CHO;
- In response to a verbal request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PII disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or
- If the official is an authorized federal official seeking PII for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to 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 and 879 (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.

PRIVACY REQUIREMENTS

All CHOs involved with the AKHMIS and / or the AK CoCs CES must comply with the privacy requirements described in this document with respect to:

- Data collection limitations;
- Data quality;
- Purpose and use limitations;
- Openness;
- Access and correction; and
- Accountability.

A CHO must comply with federal, state, and local laws that require additional confidentiality protections. All additional protections must be described in the CHO's privacy notice. A CHO must comply with all privacy protections in this Notice and with all additional privacy protections included in its privacy notice, where applicable.

A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PII. When PII is shared between organizations, responsibilities for privacy may reasonably be allocated between the organizations. Organizations sharing a common data storage medium and PII may adopt differing privacy policies as they deem appropriate, administratively feasible, and consistent with this Policy, which allows for the de-duplication of clients at-risk of or experiencing homelessness at the CoC level.

COLLECTION LIMITATION

A CHO may collect PII only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge of the individual. A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information (Alaska CoC Statewide Consumer Notice). Consent of the individual for data collection may be assumed when the Alaska CoC Statewide Consumer Notice is properly displayed according to this Policy.

DATA QUALITY

PII collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PII entered into AKHMIS should be accurate, complete, and timely, as defined by the AKHMIS Data Quality Plan. A CHO must develop and implement a plan to dispose of, or remove identifiers from, PII that is not in current use seven years after the PII was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

PURPOSE SPECIFICATION AND USE LIMITATION

A CHO may use or disclose PII only if the use or disclosure is allowed by this Policy. A CHO may assume consent for all uses and disclosures specified in this Policy and for uses and disclosures determined by the CHO to be compatible with those specified in this Policy. This Policy limits the disclosure of PII to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures not specified in this Notice can be made only with the consent of the client or when required by law.

A CHO processing PII for the purposes of the AKHMIS, and / or the AK CoCs CES will agree to additional restrictions on the use or disclosure of the client's PII at the request of the client, where it is reasonable to do so. This can include, but is not limited to, the following additional restrictions:

- Entering client PII into the AKHMIS so that it is not shared with any other CHO; or
- Using de-identified client information when coordinating services through the AK CoCs CES processes.

A CHO, in the exercise of professional judgment, will communicate with a client who has requested additional restrictions, when it is reasonable to agree to these and alternatives in situations where it is not reasonable.

OPENNESS

A CHO must adhere to this Policy describing its practices for the processing of PII and must provide a copy of this Policy to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of this Policy on the web page. A CHO must post the Alaska CoC Statewide Consumer Notice stating the availability of this Policy to any individual who requests a copy.

This Policy may be amended at any time and amendments may affect PII obtained by a CHO before the date of the change. An amendment to this Policy regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

In addition, CHOs that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the program. *See HUD Limited English Proficiency Recipient Guidance* published on December 18, 2003 (68 FR 70968).

ACCESS AND CORRECTION

In general, a CHO must allow an individual to inspect and to have a copy of any PII about the individual. A CHO must offer to explain any information that the individual may not understand. A CHO must consider any request by an individual for correction of inaccurate or incomplete PII pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

A CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PII:

- Information compiled in reasonable anticipation of litigation or comparable proceedings;
- Information about another individual (other than a health care or homeless provider);
- Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or
- Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A CHO can reject repeated or harassing requests for access or correction. A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the PII about the individual.

ACCOUNTABILITY

A CHO must establish a procedure for accepting and considering questions or complaints about this Policy. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors, and associates) to sign a confidentiality agreement that acknowledges receipt of a copy of this Policy and that pledges to comply with this Policy.

SPECIAL CONSIDERATION FOR RHY-FUNDED AND YHDP-FUNDED PROVIDERS

This section addresses special considerations for Runaway and Homeless Youth (RHY) Program and Youth Homelessness Demonstration Program (YHDP) service providers, per the YHDP Program HMIS Manual and the RHY Program HMIS Manual.

NO CONSENT REQUIRED FOR DATA COLLECTION

Data collection is the process of collecting and entering information into the AKHMIS and/ or the AK CoCs CES by RHY and YHDP program staff. All RHY and YHDP projects are required to collect specific data elements, including the HUD Universal Data Elements and program-specific data elements for the project for which they receive funding (Street Outreach Program, Basic Center Program, Transitional Living Program).

The Runaway and Homeless Youth Act requires that a RHY grantee "keep adequate statistical records profiling the youth and family members whom it serves (including youth who are not referred to out-of- home shelter services)."

RHY grantees are not required to obtain youth or parental consent to collect and enter youth data into the AKHMIS, and/or the AK CoCs CES.

CONSENT NEEDED FOR DATA SHARING

Data sharing refers to the sharing of client information per the Policy laid out in this document. For RHY and YHDP grantees, data can only be shared if written consent is obtained from the parent or legal guardian of a youth who is under age 18, or with written consent from a youth who is 18 or older.

The RHY rule states the following regarding data sharing:

Pursuant to the Act, no records containing the identity of individual youth served by a Runaway and Homeless Youth grantee may be disclosed except:

- For Basic Center Program (BCP) grants, records maintained on individual youth shall not be disclosed without the informed consent of the youth and parent or legal guardian to anyone other than another organization compiling statistical records, or a government organization involved in the disposition of criminal charges against the youth;
- For Transitional Living Programs (TLP), records maintained on individual youth shall not be disclosed without the informed consent of the youth to anyone other than an organization compiling statistical records;
- Research, evaluation, and statistical reports funded by grants provided under section 343 of the Act are allowed to be based on individual youth data, but only if such data are de-identified in ways that preclude disclosing information on identifiable youth;
- Youth served by a Runaway and Homeless Youth grantee shall have the right to review their records; to correct a record or file a statement of disagreement; and to be apprised of the individuals who have reviewed their records;
- The Department of Health and Human Services (HHS) policies regarding confidential information and experimentation and treatment shall not apply if HHS finds that state law is more protective of the rights of youth;
- Procedures shall be established for the training of RHY program staff in the protection of these rights and for the secure storage of records. 45 CFR § 1351.21.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]
- Runaway and Homeless Youth Final Rule [External link]
- YHDP Program HMIS Manual [External link]
- RHY Program HMIS Manual [External link]

2.2 RESPONSIBILITY AND IMPLEMENTATION

POLICY

The importance of the privacy and security of the AKHMIS cannot be overstated. Given this importance, the AKHMIS must be administered and operated under high standards of data privacy and security. ICA and CHOs are jointly responsible for ensuring that the AKHMIS data processing capabilities, including the collection, maintenance, use, disclosure, transmission, and destruction of data comply with the AK CoC Statewide Privacy Policy and the AK CoC Statewide Security Policy. When a privacy or security standard conflicts with other Federal, state, and local laws to which the CHO must adhere, the CHO must contact ICA to collaboratively update the applicable policies for the CHO to accurately reflect the additional protections.

REFERENCES

- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]
- Alaska CoC Statewide Privacy Policy [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

2.3 COLLECTION AND USE OF PERSONAL INFORMATION

POLICY

Pursuant to the AK CoC Statewide Privacy Policy, personal information will be collected for and entered into the AKHMIS only when it is needed to provide services, when it is needed for another specific purpose of the CHO where a client is receiving services, or when it is required by law.

Personal information may be collected, used, and disclosed for these purposes:

- To provide or coordinate services for clients;
- To find projects that may provide additional assistance to clients;
- To comply with government and grant reporting obligations;
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources.

PROCEDURE

Only lawful and fair means are used to collect personal information. All AKHMIS users must be familiar with the AK CoC Statewide Privacy Policy, which details the ways in which PII can be used and disclosed. A full copy of the AK CoC Statewide Privacy Policy is available upon client request.

Only personal information relevant for the purpose(s) for which it will be used will be collected. Personal information must be accurate and complete.

Access to client-level information in the AKHMIS by persons accessing the system (AKHMIS Users) will be restricted to the minimum level necessary to complete job duties.

Client files not used in seven years may be made inactive in the AKHMIS. Personal information may be retained for a longer period if required by statute, regulation, contract, or another obligation.

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

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

2.4 COMPLAINTS AND ACCOUNTABILITY

POLICY

Questions or complaints about the AK CoC Statewide Privacy Policy may be submitted to the CHO where the client receives services. Complaints received by the CHO specific to the AK CoC Statewide Privacy Policy should be submitted to the AKHMIS Lead Agency's Project Manager. If there is no resolution, the Executive Directors of the AK CoCs, in consultation with the AK CoCs' Executive Committees, will oversee final arbitration. All other complaints will follow the CHO's grievance procedure as outlined in the CHO's handbook.

PROCEDURE

Each CHO will have defined Grievance Procedures which will be made available to the CoC upon request.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

2.5 USE OF A COMPARABLE DATABASE BY VICTIM SERVICES PROVIDERS

POLICY

Victim services providers, private nonprofit agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, must not directly enter or provide personally identifying information in the AKHMIS if they are legally prohibited from participating in an HMIS. Victim service providers that are recipients of funds requiring participation in the HMIS but are prohibited from entering data in an HMIS, must use a comparable database to enter client information.

PROCEDURE

A comparable database is a database that can be used to collect client-level data over time and generate unduplicated aggregated reports based on the client information entered into the database. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by the AKHMIS.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]
- HMIS Comparable Database Manual [External link]

3 SECURITY

This Policy describes standards for the security of personal information collected and stored in the Alaska Homeless Management Information System (AKHMIS), as well as personal information collected for the purposes of either Alaska Continuums of Care (AK CoCs) Coordinated Entry System. The standards seek to ensure the security of personal information. This Security Policy (hereinafter referred to as "Policy") is based on principles of fair information practices recognized by the information security and technology communities.

This Policy defines the security standards that will be required of any organization within the State of Alaska that records, uses, or processes personally identifiable information (PII) on clients at-risk of or experiencing homelessness for the AKHMIS, and/or the AK CoCs CES. Organizations must also comply with federal, state, and local laws that require additional security protections, where applicable.

This Policy recognizes the broad diversity of organizations that participate in the AKHMIS, and/or the AK CoCs CES, and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations such as those serving victims of domestic violence may choose to implement higher levels of security standards because of the nature of the clients they serve and/or service provision. Others (e.g., large emergency shelters) may find higher standards overly burdensome or impractical. At a minimum, however, all organizations must meet the security standards described in this Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for organizations with additional needs or capacities.

The following sections discuss the **Alaska Continuums of Care Security Statewide Policy (AK CoC Statewide Security Policy).**

3.1 ALASKA COC STATEWIDE SECURITY POLICY (AK COC STATEWIDE SECURITY POLICY)

DEFINITIONS

Personally Identifiable Information (PII): Any information maintained by or for a Covered Homeless Organization about a client at-risk of or experiencing homelessness that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Covered Homeless Organization (CHO): Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, or processes PII on clients at-risk of or experiencing homelessness for an HMIS or CES. This definition includes both organizations that have direct access to the AKHMIS, and / or the AK CoCs CES, as well as those organizations who do not but do record, use, or process PII.

Processing: Any operation or set of operations performed on PII, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission, and destruction of the information.

SCOPE AND APPLICABILITY

This section describes the standards for system, application, and hard copy security. All CHOs must comply with these requirements.

SYSTEM SECURITY STANDARDS

Equipment Security. A CHO must apply system security provisions to all the systems where PII is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes, and servers.

User Authentication. Each user accessing a workstation that has access to AKHMIS and/or CES data must have a unique username and password to access the workstation. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

- Using at least one number and one letter or symbol;
- Not using, or including, the username, the AKHMIS name, or the HMIS vendor's name; and/or
- Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

Virus Protection. A CHO must protect the AKHMIS and any electronic device used to store PII for the purposes of the AK CoCs CES from viruses by using commercially available virus protection software.

Virus protection must include automated scanning of files as they are accessed by users on the system where the AKHMIS application is housed and/or where PII for the purposes of the AK CoCs CES is stored. A CHO must regularly update virus definitions from the software vendor.

Firewalls. A CHO must protect the AKHMIS and any electronic device used to store PII for the purposes of the AK CoCs CES from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall so long as there is a firewall between that workstation and any systems, including the Internet and other computer networks located outside of the organization.

For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall so long as the server has a firewall. Firewalls are commonly included with all new operating systems. Older operating systems can be equipped with secure firewalls that are available both commercially and for free on the Internet.

The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

Public Access. The AKHMIS and any electronic device used to store PII for the purposes of the AK CoCs CES that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates, or extranets that limit access based on the Internet Provider (IP) address, or similar means. A public forum includes systems with public access to any part of the computer through the Internet, modems, bulletin boards, public kiosks, or similar arenas.

Physical Access to Systems with Access to AKHMIS Data. A CHO must, at all times, staff computers stationed in public areas that are used to collect and store AKHMIS and/or AK CoCs CES data. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, a password-protected screensaver should automatically turn on when the workstation is temporarily not in use. Password-protected screensavers are a standard feature with most operating systems and the amount of time can be regulated by a CHO. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.

DATABASE SECURITY

Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Disaster Protection and Recovery. The AKHMIS data is copied on a regular basis to another medium (e.g., tape) and stored in a secure off-site location where the required security standards apply. The CHO that stores the data (WellSky^{TM}) in a central server stores that central server in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors are used to protect systems used for collecting and storing all the AKHMIS data.

Disposal. Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures. In order to delete all AKHMIS, and/or AK CoCs CES data from a data storage medium, a CHO must reformat the storage medium. A CHO should reformat the storage medium more thanonce before reusing or disposing the medium.

System Monitoring. A CHO must use appropriate methods to monitor security systems. Systems that have access to any AKHMIS, and/or AK CoCs CES data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely.

REPORTING SECURITY INCIDENTS

AKHMIS users and CHO Program Directors should report all unauthorized access of the AKHMIS and unauthorized attempted access of the AKHMIS. This includes theft of usernames and passwords. Security incidents should be reported to ICA. ICA will use the AKHMIS user audit trail report to determine the extent of the breach of security.

All AKHMIS users must be familiar with the AK CoC Statewide Security Policy which fully explains the security requirements of the AKHMIS. A full copy of the AK CoC Statewide Security Policy is available upon client request.

APPLICATION SECURITY STANDARDS

These provisions apply to how all AKHMIS data are secured by the HMIS application software.

Applicability. A CHO must apply application security provisions to the software during data entry, storage, and review or any other processing function.

APPLICATION SECURITY

AKHMIS users will be assigned a system access level that restricts their access to appropriate data.

User Authentication. A CHO must secure all electronic AKHMIS, and/or AK CoCs CES data with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

Using at least one number and one letter or symbol;

Not using, or including, the username, the AKHMIS name, or the HMIS vendor's name; and

Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users should not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

Vendor User Authentication. Users may only access the AKHMIS with a valid username and password combination that is encrypted via SSL for internet transmission to prevent theft. If a user enters an invalid password three consecutive times, they are automatically shut out of that AKHMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Electronic Data Transmission. A CHO must encrypt all AKHMIS, and / or AK CoCs CES data that are electronically transmitted over the Internet, publicly accessible networks, or phone lines to current industry standards. The current standard is 128-bit encryption. Unencrypted data may be transmitted over secure direct connections between two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data. A secure network would have secure direct connections.

Electronic Data Storage. A CHO must store all AKHMIS, and / or AK CoCs CES data in a binary, not text, format. A CHO that uses one of several common applications (e.g., Microsoft Access, Microsoft SQL Server, or Oracle) are already storing data in binary format and no other steps need to be taken.

HARD COPY SECURITY STANDARDS

This section provides standards for securing hard copy data.

Applicability. A CHO must secure any paper or other hard copy containing PII that is either generated by or for the AKHMIS, and / or AK CoCs CES, including, but not limited to reports, data entry forms, and case / client notes.

Security. A CHO must, at all times, supervise any paper or other hard copy generated by or for the AKHMIS, and / or the AK CoCs CES that contains PII when the hard copy is in a public area. When CHO staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location. Any hard copy that contains PII must be shredded upon disposal.

REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

3.2 CLASSIFICATION OF DATA

POLICY

All AKHMIS data will be handled according to the following two major classifications: Open Data (with two subclasses of Open Public Data and Open Restricted Data) and Confidential Data.

PROCEDURE

CLASSIFICATIONS OF DATA

Open Data: Does not include personally identifiable information (PII).

- **Open Public Data (aggregate)** – Aggregate data only, with no client-level information. Data cannot be traced back to any client.
- **Open Restricted Data (client-level)** – De-identified data (PII has been removed) with multiple elements of information available per client. Data cannot be traced back to any client.

Confidential Data (client-level, identifying): Data that contain personally identifiable information (PII).

REFERENCES

- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]
- Access to Data/Data Sharing within HMIS [AKHMIS Policy: Internal link]

3.3 ACCESS TO DATA

POLICY

ICA staff will implement controls to ensure that confidential data are appropriately accessible to AKHMIS users at Covered Homeless Organizations (CHOs). Users needing access to confidential data in AKHMIS will have the level of access necessary to fulfill their job duties, and all other access will be restricted.

PROCEDURE

Users are granted access to shared data within AKHMIS, and to unshared data within projects at their own organization. Users are only given access to the projects (and the data within those projects) as it is required to complete their job duties.

Read-only user licenses are not allowable in AKHMIS. AKHMIS user licenses are assigned to users whose job duties fit one or more AKHMIS User Levels, in alignment with the Alaska HMIS Privacy Policy.

Users may be granted access to projects outside of their own organization (and the data within those projects) through a Coordinated Services Agreement (CSA).

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

3.4 COORDINATED SERVICES AGREEMENT DATA SHARING

POLICY

A Coordinated Services Agreement (CSA) allows an AKHMIS user from a CHO to access and enter client-level data (including confidential data) into AKHMIS on behalf of a different CHO and/or to report client-level data on behalf of the different CHO. A CSA must be in place before a user may access any data that is not within their own organization.

PROCEDURE

A CSA must be signed by the Executive Director of each CHO involved in the CSA. A user will only have access to the projects (and the data within those projects) that are included on the CSA.

If a user under a CSA is not compliant, or an organization with a CSA is not compliant, the AKHMIS Operating Policies Violation policy and procedure will apply.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]
- AKHMIS Operating Policies Violation [AKHMIS Policy: Internal link]

3.5 DATA SHARING WITHIN AKHMIS

POLICY

AKHMIS data will be accessible to users within AKHMIS according to the following major classifications: Shared Data and Unshared Data. ICA staff will assess and implement controls to ensure that data are appropriately accessible in AKHMIS.

PROCEDURE

ICA staff will ensure projects are set up in the AKHMIS to provide for the levels of record sharing indicated below:

Shared Data: Unrestricted information that has been entered by one Covered Homeless Organization (CHO) and is visible/is accessible to other CHOs with access to the AKHMIS for the uses and disclosures laid out in the AK CoC Statewide Privacy Policy.

Shared data can also include data that is disclosed from the AKHMIS for the purposes laid out in the AK CoC Statewide Privacy Policy.

Additionally, individual client records can be unshared at the client's request.

Unshared Data: Information entered into the AKHMIS by one Covered Homeless Organization that is not visible to other Covered Homeless Organizations accessing the AKHMIS.

Programs that are funded by the Runaway and Homeless Youth (RHY) program and/or Youth Homelessness Demonstration Program (YHDP) will not share data, unless they receive written consent from the youth or the underage youth's parent or legal guardian, per the AK CoC Statewide Privacy Policy.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]

3.6 COMMUNICATION/TRANSMISSION OF DATA

POLICY

Each Covered Homeless Organization (CHO) shall develop rules concerning AKHMIS data to ensure data are transmitted or communicated so that privacy is maintained and that the proper controls are in place to ensure data are handled appropriately according to the data classification. Confidential data should only be transmitted if necessary. Recipients of confidential data are responsible for protecting these data as per the organization's policies for confidential data.

PROCEDURE

Open Public Data (aggregate) – These data may be made publicly available according to "Principles for Data Release". Security controls are not required.

Open Restricted Data (client-level) – These data should have security controls in place to limit access and transmission; transmission may be undertaken without encryption when made available directly to appropriate recipients.

Confidential Data (client-level, identifying) – If there is a need to share or reference confidential data (client-level, identifying information) and verbal methods are unavailable, only a client file number may be shared via email. No confidential data may be transmitted via email unless the file is securely encrypted or sent via encrypted email message and only available for decryption by appropriate recipients.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

3.7 STORAGE/DESTRUCTION OF DATA

POLICY

Each Covered Homeless Organization (CHO) shall develop rules regarding the storage and destruction of hard copy and electronic AKHMIS data to ensure that privacy is maintained and that proper controls are in place to secure AKHMIS data to the extent necessary according to the data classification. Confidential AKHMIS data should only be stored outside of AKHMIS if necessary. Confidential data outside of AKHMIS must be secured at all times, in either physical or electronic format.

PROCEDURE

Open Public Data (aggregate) – Further security controls are not required.

Open Restricted Data (client-level) – These data should be handled discretely and stored out of sight, with limited access to both hard and electronic copies.

Confidential Data (client-level, identifying) – Hard copies shall be stored in a secure environment that is inaccessible to the general public or staff not requiring access. Hard copies shall not be left out in the open or unattended. Hard copies shall be shredded when disposal is necessary.

Electronic copies shall be stored only where the employee can access the data. Electronic copies shall be stored where a password is required to access the data. Electronic copies require encryption at all times, unless being appropriately accessed. Electronic copies must be magnetically overwritten and physically destroyed for disposal.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

3.8 PRINCIPLES FOR REPORTING

In accordance with the Purpose Specification and Use Limitation in the AK CoC Statewide Privacy Policy:

- No more than the minimum amount of data necessary to fulfill reporting requirements will be used or released within any report.
- If at all possible, de-identified aggregate information will be used or released within any report.
    - Aggregate reports will be generated in accordance with all AKHMIS data use policies.
    - If data are made publicly available, those data will be de-identifiedidentified and in aggregated form.
- ICA reserves the right to deny any request for aggregate data.
- Personally identifying information (PII) will not be released in reports for uses or disclosures not specified in the AK CoC Statewide Privacy Policy without client consent.
- Program-specific information used for annual grant program reports and program-specific information included in grant applications is classified as public information. No other program-specific information will be released without prior approval.

3.9 REPORTING WITH CLIENT NAMES

POLICY

Any report that discloses confidential data including client names will have a disclaimer at the top to notify those in possession of the report of that personally identifying information (PII) is contained within and to indicate their responsibility to protect the report's contents according to AKHMIS policies and their organization's policies for handling PII.

PROCEDURE

A report that includes client names will have warning text included at the top of EACH tab that contains confidential information.

Recipients of are responsible for protecting these data in accordance with the AKHMIS Data Storage/Destruction of Data Policy and as per the organization's policies for confidential data.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]
- Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements [External link]
- Storage/ Destruction of Data [AKHMIS Policy: Internal link]

3.10 DATA REPORTING REQUESTS

POLICY

Requests for data and/or reports will be evaluated and fulfilled on a case-by-case basis.

Requests by Covered Homeless Organizations (CHOs) for any of their own data at any level of detail do not require any approval and will be fulfilled as per current reporting practices. Requests for **Open Data** other than requests by a CHO for its own data may be subject to AK CoC approval before being fulfilled. Requests for **Confidential Data** other than a CHO requesting their own data will not be fulfilled without a Data Use Agreement (DUA) or equivalent agreement in place.

ICA reserves the right to require the approval of both AK CoC Directors before fulfilling any data request.

POSSIBLE INCLUSIONS/REPLACEMENTS FOR THE ABOVE:

Requests for **Open Public Data at the system level** do not require AK CoC approval.

Requests for **Open Public Data at the agency-, program-, or project-level** by made by an AK CoC Committee for the purposes of system performance evaluation do not require AK CoC approval.

Requests for **Open Public Data at the agency-, program-, or project-level** by an entity other than a request by a CHO for its own data or an AK CoC Committee are subject to AK CoC approval.

Requests for **Open Restricted Data** by an entity other than a request by a CHO for its own data are subject to CoC approval.

PROCEDURE

REQUESTS

Requests must be written with a description of specific data to be included and for what duration of time. Requests are to be submitted at least 45 days prior to the date the report is needed. Exceptions to the 45-day notice may be made and will be communicated to the requestee by ICA.

For data/report requests requiring AK CoC approval, the reporting team will notify their manager or management team and reach out to the manager and/or AK CoC to obtain approval before proceeding.

CASES FOR COC APPROVAL

Approval by the AK CoC Director(s) of the CoC(s) containing the data to be released is required for, but not limited to, the following cases:

1. Any request (other than a CHO requesting their own data) for Confidential Data
    a. Request involving Confidential Data also require a Data Use Agreement (DUA) or equivalent agreement
2. Any request from an agency or entity external to the AK CoCs
3. A CHO requests data outside of their own projects' data, at project-or agency-level
4. An AK CoC committee requests Open Restricted Data
5. A funder requests client-level data, whether identifying information is or is not included
6. A funder requests project-level data on a project they do not fund, whether identifying information is or is not included.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

3.11 DATA USE AGREEMENTS

POLICY

Any request for Confidential Data (client-level, identifying information) from an entity that is NOT the entity entering the data into AKHMIS will require a Data Use Agreement (DUA) signed by ICA and the recipient entity. A DUA must be entered into between ICA and the recipient organization before any data will be released. All DUAs must be approved by the AK CoC Director(s) of the CoC(s) containing the data to be released.

PROCEDURE

A DUA must include the following information:

- Identification of the recipient entity;
- Parameters of the data to be provided;
- Describe the terms and conditions of data use (including limitations of use);
- Describe the data transfer, storage, access, retention, and destruction requirements to be met and/or upheld by the parties signed to the agreement; and
- Signatures of ICA and the recipient entity.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
  2004 HMIS Data and Technical Standards Final Notice [External link]

3.12 RELEASE OF DATA FOR GRANT FUNDERS

POLICY

Entities providing funding to agencies or programs required to use the AKHMIS will not have automatic access to AKHMIS data or client-level reports. Access to the AKHMIS will only be granted by ICA when there is a voluntary written agreement in place between the funding entity and the CHO or project, and in consultation with the AK CoCs. Funding for any CHO or project using the AKHMIS cannot be contingent upon establishing a voluntary written agreement to allow the funder access to AKHMIS.

PROCEDURE

The funding entity must obtain voluntary written agreement with all grant recipients, and reporting access will be limited to only these agencies that have signed agreements.

If systemwide reports are necessary for funders, ICA will complete those reports abiding to the standard reporting timelines and CoC approval requirements.

REFERENCES

- Alaska CoC Statewide Privacy Policy [External link]
- Alaska CoC Statewide Security Policy [External link]
- Alaska CoC Statewide Consumer Notice [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

3.13 AKHMIS USER ELIGIBILITY

POLICY

AKHMIS users must be paid staff, contract worker, or official volunteers of a CHO.

PROCEDURE

The Organization shall conduct criminal background checks on all staff, contract workers, and official volunteers before requiring potential users to attend new user training led by ICA. Individuals with a history of perpetrating fraud, identity theft, or misuse of confidential information, or an individual who is under investigation for such issues, shall not be permitted an AKHMIS user license. All users must be at least 18 years old.

An official volunteer must complete a volunteer application with the CHO, undergo Organization training, pass a criminal background check, and record volunteer hours with the Organization.

REFERENCES

- Access to Data/Data Sharing within HMIS [AKHMIS Policy: Internal link]
- User Access to AKHMIS [AKHMIS Policy: Internal link]
- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]

3.14 USER ACCESS TO AKHMIS

POLICY

The ICA will determine user access for users and assign AKHMIS user licenses to the appropriate CHO. AKHMIS User licenses are assigned based on the successful completion of the required AKHMIS training(s).

PROCEDURE

All users must successfully complete all required training before ICA grants access to the AKHMIS. All AKHMIS training curricula is customized by ICA to meet each user's AKHMIS access needs. Each user's access in the AKHMIS is determined in accordance with the training they completed. Access to client-level information in the AKHMIS by users will be restricted to the minimum level necessary to complete job duties.

Read-only user licenses are not allowable in AKHMIS. AKHMIS user licenses are assigned to users whose job duties fit one or more AKHMIS User Levels, in alignment with the Alaska HMIS Privacy Policy.

If a user needs access to a project with a different CHO, a Coordinated Services Agreement must be signed by both CHO's prior to the user's access to that project.

REFERENCES

- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]
- AKHMIS Coordinated Services Agreement [External link]
- Access to Data/Data Sharing within HMIS [AKHMIS Policy: Internal link]
- AKHMIS User Eligibility [AKHMIS Policy: Internal link]

3.15 PASSWORDS

POLICY

ICA will generate usernames and passwords within the administrative function of the software. Each user accessing the AKHMIS must have his / her own username and password to access the system – sharing of usernames and passwords is forbidden.

PROCEDURE

Creation. Passwords are automatically generated from the AKHMIS when a user is created. ICA will communicate the system-generated password to the user.

Use. The user will be required to change the password the first time they log into the AKHMIS. The password must be at least eight characters and include one number and one letter or symbol. Passwords should not be able to be easily guessed or found in a dictionary. Passwords are the individual's responsibility and AKHMIS users cannot share passwords. Users may not keep written copies of their password in a publicly accessible location.

Storage. Any passwords that are written down are to be stored securely and must be inaccessible to other persons. Users are not to auto-save passwords on a personal computer for easier login.

Expiration. Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until two password selections have expired.

Unsuccessful logon. If a user unsuccessfully attempts to login three times, the User ID will be "locked out," and access permission will be revoked rendering the user unable to gain access until his / her password is reset by ICA.

REFERENCES

- AKHMIS User Agreement [External link]
- AKHMIS Coordinated Services Agreement [External link]
- Alaska CoC Statewide Security Policy [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

3.16 TRACKING OF UNAUTHORIZED ACCESS

POLICY

As the HMIS Lead Agency, it is the responsibility of ICA to maintain the AKHMIS, including protecting the data contained in the AKHMIS.

PROCEDURE

Any suspicion of unauthorized activity should be reported in writing to ICA (AKHMIS@icalliances.org).

ICA will notify the appropriate AK CoC of security issues in writing.

REFERENCES

- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]
- AKHMIS Coordinated Services Agreement [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]
- AKHMIS Operating Policies Violation

3.17 DISASTER RECOVERY PLAN

POLICY

WellSky Community Services™ Disaster Recovery Plan

The AKHMIS is covered under WellSky Community Services™ Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. To ensure service reliability, WellSky Community Services™ provides the following disaster recovery plan. Plan highlights include:

- Database tape backups occur nightly;
- Tape backups are stored offsite;
- Seven-day backup history is stored locally on instantly accessible Raid 10 storage;
- One-month backup history is stored off site;
- Access to WellSky Community ServicesTM emergency line to provide assistance related to "outages" or "downtime" 24 hours a day;
- Data is backed up locally on instantly-accessible disk storage every 24 hours;
- The application server is backed up offsite, out-of-state, on a different internet provider and on a separate electrical grid via secured Virtual Private Network (VPN) connection;
- Backups of the application site are near-instantaneous (no files older than five minutes);
- The database is replicated nightly at an offsite location in case of a primary data center failure;
- Priority level response (ensures downtime will not exceed four hours).

Standard Data Recovery

The AKHMIS database is stored online and is readily accessible for approximately 24 hours a day. Tape backups of the database are kept for approximately one month. Upon recognition of a system failure, AKHMIS can be copied to a standby server. The database can be restored, and the site recreated within three to four hours if online backups are accessible. As a rule, a tape restoration can be made within six to eight hours. On-site backups are made once daily. A restore of this backup may incur some data loss between when the backup was made andwhen the system failure occurred.

All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary core routers are configured with redundant power supplies and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that are connected in turn to electrical circuits, which are connected to a building generator.

All client data is backed-up online and stored on a central file server repository for 24 hours. Each night a tape backup is made of the client database and secured in a bankvault.

Historical data can be restored from tape as long as the data requested is newer than 30 days old. As a rule, the data can be restored to a standby server within four hours without affecting the current live site. Data can then be selectively queried and / or restored to the livesite.

For power outage, AKHMIS is backed up via APC battery back-up units, which are connected via generator-backed up electrical circuits. For a system crash, a system restore will take four hours. There is potential for some small data loss (data that was entered between thelast backup and when the failure occurred) if a tape restore is necessary. If the failure is not hard drive related, the data restore time will possibly be shorter as the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of WellSky Community Services^{TM} executive management. WellSky Community Services^{TM} support staff help manage communication or messaging to ICA as progress is made to address the service outage.

PROCEDURE

AKHMIS Disaster Recovery Plan

ICA operates a regional approach to administering HMIS implementations. The main ICA HMIS office is in Des Moines, Iowa, and there are nine regional offices located throughout the United States. In the event of a localized emergency or disaster, ICA will shift responsibility for administering the AKHMIS and managing day-to-day operations of the system to an unaffected site.

4 DATA QUALITY

Data quality is the extent to which the information contained in AKHMIS accurately represents the real-world clients and situations it is meant to describe. Components of data quality include completeness, timeliness, accuracy, consistency, coverage, and utilization.

The AK CoCs work will with ICA to ensure all projects have access to the tools they need to achieve high data quality. This includes training and data quality reports for monitoring, as well as incentives to maintain a high level of data quality and accountability for non-responsiveness to data quality concerns.

4.1 DATA QUALITY PLAN

POLICY

The AKHMIS Data Quality Plan provides actionable, measurable steps to address data quality within the Alaska Homeless Management Information System (AKHMIS), which includes both HUD-defined Alaska CoCs: Anchorage (AK-500) and Balance of State (AK-501).

PROCEDURE

The AKHMIS Data Quality Plan identifies the data entered into AKHMIS and explain the quality standards and goals set forth by the AK CoCs for these data.

The plan addresses the various components of data quality – completeness, timeliness, accuracy, consistency, coverage, and utilization – and provides the standards (minimum requirements) that AKHMIS-participating organizations entering data into AKHMIS must meet.

The plan provides how data quality will be monitored and how the AK CoCs will incentivize and enforce these standards.

The plan addresses project monitoring and provides an outline of a Data Quality Improvement Plan for use in situations where an organization's data quality consistently has room for improvement and the organization requires extra assistance to meet data quality standards.

The AKHMIS Data Quality Plan sets expectations for the AK CoCs, the Institute for Community Alliances (ICA) as the HMIS Lead, participating organizations, and AKHMIS users to ensure valid and reliable data is captured on all persons accessing homelessness services in the state of Alaska.

All organizations participating in AKHMIS will be required to sign a AKHMIS Data Quality Plan Participating Organization Agreement for access to AKHMIS. This Agreement will require the organization to participate in and abide by the processes and standards provided within the AKHMIS Data Quality Plan.

After August 27, 2018, *all new enrollments* into a project in AKHMIS are given enrollments using a Client ID of greater than 500000.

REFERENCES

- AKHMIS Data Quality Plan [External link]
- HMIS Data Standards [External link]
- CoC Program HMIS Manual [External link]
- ESG Program HMIS Manual [External link]
- YHDP HMIS Manual [External link]
- PATH Program HMIS Manual [External link]
- HOPWA Program HMIS Manual [External link]
- HUD-VASH Program HMIS Manual [External link]
- VA Programs HMIS Manual [External link]
- RHY Program HMIS Manual [External link]

4.2 MINIMUM DATA COLLECTION STANDARD

POLICY

CHOs are responsible for asking all clients a minimum set of questions for use in aggregate analysis. The required data elements depend on the CHO's project and / or funding source.

The Alaska Specific Data Elements, as designed by the Alaska CoCs, collect information that is important to Alaska-specific organizations that address and provide funding for Alaska-specific issues. The data elements were created to provide for the data collection necessary to fulfill the reporting requirements of these Alaska-specific programs, to ensure that homeless services organizations can continue to secure this funding.

PROCEDURE

These questions are included in custom assessments that are created by ICA.

CHOs are responsible for asking all clients a minimum set of questions for use in aggregate analysis. These questions are included in custom assessments that are created by ICA. The required data elements depend on the CHO's project and / or funding source. AKHMIS participating organizations are responsible for ensuring that their users are aware of the data elements that are required to be entered into the AKHMIS for their specific project(s).

A CHO's project must complete at least an average score that meets the Data Completeness Standards set in the AKHMIS Data Quality Plan of all universal and project-specific data elements to be considered meeting the minimum data collection standard. Exceptions to this standard may be granted based upon established program standards or grant requirements, such as those enumerated by federal agencies.

Guidelines clearly articulating the current mandatory expectations for data entry for all projects entering data in the AKHMIS are sent to CHO Program Directors and posted on the ICA AKHMIS webpage. Program Directors must ensure that the current mandatory universal and program-specific data elements are fulfilled for every project.

REFERENCES

- AKHMIS Data Quality Plan [External link]
- HMIS Data Standards [External link]
- CoC Program HMIS Manual [External link]
- ESG Program HMIS Manual [External link]
- YHDP HMIS Manual [External link]
- PATH Program HMIS Manual [External link]
- HOPWA Program HMIS Manual [External link]
- HUD-VASH Program HMIS Manual [External link]
- VA Programs HMIS Manual [External link]
- RHY Program HMIS Manual [External link]

4.3 MINIMUM DATA QUALITY STANDARD

POLICY

All federally funded homeless services projects are required to use AKHMIS and must meet certain data quality expectations to ensure accurate reporting for those grants. However, as all providers that enter data into the AKHMIS contribute to the overall picture of homelessness within the state of Alaska, all providers will be expected to participate in this AKHMIS Data Quality Plan, regardless of funding source.

PROCEDURE

All organizations participating in AKHMIS will be required to sign a AKHMIS Data Quality Participating Organization Agreement for access to AKHMIS. This Agreement will require the organization to participate in and abide by the processes and standards provided within the AKHMIS Data Quality Plan.

CHOs are responsible for the overall quality, accuracy, and completeness of data entered by their staff for the clients served by their projects in the AKHMIS. ICA staff will monitor data collection of the HMIS Universal Data Elements and required program-specific data elements in accordance with the process laid out in the AKHMIS Data Quality Plan – Section 5 Alaska HMIS Project Data Quality Standards and Policy 4.1 Data Quality Monitoring.

CHOs will be responsive to requests from ICA to confirm data entered into the AKHMIS is complete, accurate, and timely, and will make changes as appropriate to meet system requirements. Unresponsive organizations will be referred to the Executive Directors of the AK CoCs forreview.

ICA will submit a report to the AK CoCs quarterly that identifies the degree to which all CHOs within the CoCs are meeting the minimum data entry standards.

A Data Quality Improvement Plan may be advised when the quarterly data quality reports document one or more ongoing improvement opportunities related to data quality within a given organization (i.e., ongoing is defined as the improvement opportunity lasting longer than a specific period of time as defined by the AK CoC and ICA without resolution). Organizations that continue to demonstrate a complete inability to meet minimum data quality standards and a lack of engagement may have their AKHMIS access suspended, at the discretion of the CoC to preserve the integrity of AKHMIS and ensure that other organizations do not suffer due to poor data quality from another organization.

REFERENCES

- AKHMIS Data Quality Plan [External link]
- HMIS Data Standards [External link]
- CoC Program HMIS Manual [External link]
- ESG Program HMIS Manual [External link]
- YHDP HMIS Manual [External link]
- PATH Program HMIS Manual [External link]
- HOPWA Program HMIS Manual [External link]
- HUD-VASH Program HMIS Manual [External link]
- VA Programs HMIS Manual [External link]
- RHY Program HMIS Manual [External link]

4.4 DATA ENTRY TIMELINESS STANDARD

POLICY

CHOs participating in the AKHMIS must meet the current mandatory data entry requirements established by the AKHMIS Data Quality Plan as well as those set forth by the entities funding their projects, including by HUD and its federal partners, as well as any updates to standards set forth by the local, state, or federal government.

PROCEDURE

Data must be entered within the timelines set for in the AKHMIS Data Quality Plan – 5.3 Timeliness.

REFERENCES

- AKHMIS Data Quality Plan [External link]
- HMIS Data Standards [External link]

4.5 BED COVERAGE UPDATES

POLICY

The AK CoCs will review and update the CoCs' most recent Housing Inventory Chart (HIC) to know which projects participated in the most recent HIC but are not entering data into HMIS (excluding Victim Services Projects) on a quarterly or semi-annual basis.

PROCEDURE

The AK CoCs will ensure that bed coverage is as close to 100% as is possible for applicable project types, and the AK CoCs will focus on project types with less than 85% bed coverage for improvement efforts.

This procedure is under development.

REFERENCES

- AKHMIS Governance Charter [External link]
- AKHMIS Data Quality Plan [External link]
- HMIS Data Standards [External link]

4.6 ADDITIONAL DATA ELEMENTS

POLICY

CHOs may collect information for data elements in addition to the minimally required data elements recommended by the AKHMIS Advisory Board and approved by the AK CoCs' Executive Committees, in accordance with HUD. CHOs must maintain consistency with data collection and entry within each project.

PROCEDURE

To request a new data element to be collected by all organizations entering data into AKHMIS across Alaska.

> *NOTE: This process is NOT for when an organization/project wants to add a data field only for themselves or a single project; that is accomplished by submission of a Help Desk work ticket.*

1. Organizations will submit a New Alaska Specific Data Element Request ("Request") to the AKHMIS Advisory Board Chair.
    a. Requests will be accepted by AKHMIS Advisory Board Chair throughout the year until ***April 15.*** Requests received after April 15 will be included in the vetting process for the following year.
    b. Requests will be vetted at the May AKHMIS Advisory Board Meeting.
2. At the ***May*** AKHMIS Advisory Board Meeting, the AKHMIS Advisory Board will approve or deny a Request based on the following:
    a. What value would the New Alaska Specific Data Element provide to organizations entering data into AKHMIS? To the CoC?
    b. Will clients served by organizations entering data into AKHMIS be willing to provide the information being requested?
    c. Is collection of the data element possible and not an undue burden on organizations?
3. The AKHMIS Advisory Board Chair will submit all approved Requests to both Alaska CoCs for approval ***within three business days*** of the May AKHMIS Advisory Board meeting.
4. Each Alaska CoC will notify the AKHMIS Advisory Board of their approval/denial of Requests received by ***June 30***.
5. If a Request has been approved by both Alaska CoCs, the AKHMIS Advisory Board will notify the requestor and ICA.
6. The requestor will work with the AKHMIS Advisory Board and ICA to complete the following tasks by ***August 15***:
    a. Create the assessment to collect the data element in AKHMIS;
    b. Develop a reporting tool for the data element; and
    c. Develop training materials for the collection and entry of the new data element in AKHMIS.
7. ICA will prepare and then provide training on the new Alaska Specific Data Element in ***September***, along with training for any other HUD HMIS updates.
8. The new Alaska Specific Data Element, along with any other HUD HMIS updates, will be effective in AKHMIS on ***October 1***.

REFERENCES

- Request for New or Altered Alaska Specific Data Element Form

4.7 XML IMPORTS

POLICY

While HMIS databases are required to have the capacity to accept XML imports, ICA reserves the right to not allow XML imports into the AKHMIS. Allowing XML imports can impact data integrity and increase the likelihood of duplication of client files in the system.

PROCEDURE

If a request for this occurs, ICA will work with the Executive Directors of the AK CoCs and WellSky Community Services^{TM} to determine the feasibility of an XML import into the AKHMIS taking into account cost, time, and impact on data quality.

5 MONITORING

5.1 DATA QUALITY MONITORING

POLICY

Ongoing AKHMIS data quality monitoring will be conducted with the goal of ensuring that AKHMIS-participating organizations maintain a high level of data quality at all times with a minimal amount of data clean-up. The AK CoCs will work with ICA to monitor data quality.

PROCEDURE

LEVEL ONE: AKHMIS-PARTICIPATING ORGANIZATION DATA MANAGEMENT

Responsibility: AKHMIS-participating organizations (including HMIS Users)

1. AKHMIS-participating organizations understand the AKHMIS Data Quality Plan. If the AKHMIS-participating organization/user is not familiar with the AKHMIS Data Quality Plan, it is a good opportunity to read and become familiar with the Alaska standards and goals.
2. AKHMIS-participating organizations enter accurate and complete data in a timely manner. AKHMIS-participating Organizations are expected to be routinely entering and updating data in AKHMIS. The AKHMIS Data Quality Plan defines the data standards that must be met. See the AKHMIS Data Quality Plan.
3. AKHMIS-participating organizations review reports regularly to ensure data is entered accurately and completely**.** Data reports should be generated or can be requested from ICA using the quarterly start and end dates, or dates as determined by the AKHMIS-participating organization. Visual Guides for AKHMIS-participating organizations to run their own reports are available in the How-To Guides folder on the ICA Website Folder. The password to access the page is: “alaska”.

LEVEL TWO: ALASKA HMIS SYSTEM QUARTERLY MONITORING

1. Run and email AKHMIS Data Quality Reports

   Responsibility: AK CoC, ICA, and AKHMIS-participating organizations (including HMIS Users)

   A. ICA runs data monitoring reports for projects and emails to AK CoCs and AKHMIS-participating organizations.
   B. The AK CoCs reviews report prompts, provider lists, and reports.
   C. The AK CoCs and ICA contacts AKHMIS-participating organizations regarding the data quality reports, particularly if the report includes data quality errors.

2. Step 2: Review and correct missing data or errors

   Responsibility: AKHMIS-participating organizations (including HMIS Users)

   A. An AKHMIS-participating organization with an identified data quality improvement opportunity is permitted a minimum of one month to correct their data or processes.
      1) AKHMIS-participating organizations will follow any instructions laid out in the email sent by AK CoC and/or ICA.
      2) AKHMIS-participating organizations will review the reports and make corrections for identified errors within one month of receiving the reports.
   B. If the AKHMIS-participating organization is unable to make the corrections within the month timeframe, the AKHMIS-participating organization is responsible for contacting the AK CoC and ICA in writing to advise them of the delay and the expected completion date.

C. AKHMIS-participating organizations will run the appropriate reports for their projects to verify corrections have been made. Visual Guides for running reports are available in the How-To Guides folder on the ICA Website Folder. The password to access the page is: "alaska".

3. Re-run and email Data Quality Reports

Responsibility: AK CoCs, ICA and AKHMIS-participating organizations (including AKMIS Users)

A. After the deadline for data correction for the quarter has passed, ICA re-runs data monitoring reports and emails to AK CoC and AKHMIS-participating organizations.
B. AK CoC and/or ICA contacts AKHMIS-participating organizations to repeat the process and ensure data is complete, accurate, and timely.

LEVEL THREE: ALASKA HMIS PROGRESS MONITORING

1. Progress Reports

Responsibility: ICA

- ICA will provide a list of projects that have not improved their data and/or still below the standard benchmarks to the AK CoCs and AKHMIS-participating organizations.
- ICA will also provide a list of projects to the AK CoC that have not improved their data since the previous quarter, or who have had multiple quarters with insufficient progress.
- ICA will provide Data Quality Progress Reports to the CoC quarterly.

2. Ongoing Evaluation and DQIP

Responsibility: AK CoCs, ICA, CoC and AKHMIS-participating organizations (including AKHMIS Users)

A. For persistent data quality issues, AKHMIS-participating organizations may be contacted by the AK CoC to discuss the implementation of a Data Quality Improvement Plan (DQIP) (see 8.3 Data Quality Improvement Plan) for the project(s).
B. If a project's data quality does not improve over two consecutive quarters:
    1) The AK CoC contacts the AKHMIS-participating organization who may be advised to develop a Data Quality Improvement Plan, which is a detailed work plan intended to support and enhance a project's data quality in a specific area.
    2) ICA offers walkthrough support.
C. If a project's data quality does not improve over three consecutive quarters:
    1) AK CoC contacts the AKHMIS participating organization who will be advised to develop a Data Quality Improvement Plan, which is a detailed work plan intended to support and enhance project's data quality in a specific area.
    2) ICA identifies which users require additional training.
D. If a project's data quality does not improve over five quarters out of eight:
    1) AK CoC to determine appropriate action.
    2) Potential for lost points on AK CoC competition or similar consequence.
    3) Increased monitoring.
    4) The AK CoC and ICA may offer additional support and/or training to the AKHMIS participating organization until such a time as the AKHMIS-participating organization effectively demonstrates an ability to meet with minimum data entry standards. Determination of ability is at the discretion of the AK CoC.

DATA QUALITY PROGRESS CHART

ICA will provide the AK CoCs with quarterly progress reports.

DATA QUALITY EXPECTATIONS

Quarterly Correction Expectation. Ongoing AKHMIS data quality monitoring will be conducted quarterly. Data quality issues that are the result of problems with a data entry process will be noticed more quickly with regular monitoring, which means corrections to processes can be implemented earlier to minimize the amount of corrections that will be necessary. Additionally, it can be easier to make corrections to more recent records where a client is still available and/or before a problem is compounded by information added at a later date.

Due Dates. The due dates for an AKHMIS-participating organization's quarterly corrections will be determined on a case-by-case basis with the AKHMIS-participating organization.

REFERENCES

- AKHMIS Governance Charter [External link]
- AKHMIS Data Quality Plan [External link]
- HMIS Data Standards [External link]
- CoC Program HMIS Manual [External link]
- ESG Program HMIS Manual [External link]
- YHDP HMIS Manual [External link]
- PATH Program HMIS Manual [External link]
- HOPWA Program HMIS Manual [External link]
- HUD-VASH Program HMIS Manual [External link]
- VA Programs HMIS Manual [External link]
- RHY Program HMIS Manual [External link]

5.2 ORGANIZATION COMPLIANCE MONITORING

POLICY

The AK CoCs and ICA will evaluate how compliant an organization is for entering data into AKHMIS, following AKHMIS policies and procedures, organization agreements, user agreements, and any other documents governing the use of AKHMIS.

PROCEDURE

The CoCs will use a standard AKHMIS Annual Monitoring Tool to evaluate how compliant an organization entering data into AKHMIS is with this Data Quality Plan, AKHMIS policies and procedures, organization agreements, user agreements, and any other documents governing the use of AKHMIS.

The AK CoCs will follow the evaluation process set forth in the AKHMIS Data Quality Plan - Section 8. Data Quality Improvement.

REFERENCES

- AKHMIS Governance Charter [External link]
- AKHMIS Data Quality Plan [External link]
- AKHMIS Data Quality Plan Participating Organization Agreement [External link]
- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]
- AKHMIS Coordinated Services Agreement [External link]

5.3 PROGRAM NONCOMPLIANCE REPORTING

POLICY

When Partner Organizations are out of compliance with HUD standards ICA, the AKMIS Advisory Board or any other party who becomes aware of the issue will immediately notify the applicable CoC.

PROCEDURE

The party who becomes aware of the issue will immediately send written notification of noncompliance to the applicable CoC and ICA.

REFERENCES

- AKHMIS Governance Charter [External link]

6 AKHMIS SYSTEM ADMINISTRATION

POLICY

ICA, as the HMIS Lead, is responsible for the system administration of AKHMIS.

PROCEDURE

There are generally six basic roles related to the AKHMIS and its data. These are:

Project management. Oversees the general management of the AKHMIS project. Usually interacts with the AK CoC's leadership and program leadership. Identify AKHMIS software issues and to identify user training needs. Maintain all AKHMIS policies, procedures, and protocols for functions essential to the viability and success of the AKHMIS including, but not limited to operational agreements, data privacy, data quality, analysis, reporting, and data sharing protocols.

System administration. Manages the technical aspects of the day-to-day operations of the AKHMIS. Works directly with the users and the HMIS software vendor to ensure authorized access to client information, accessibility of the AKHMIS software, software performance, correct set up and monitoring of system security, and adherence to the AK CoC Privacy Policies within the software. Responsible for the activities and tasks outlined in the HUD HMIS System Administrator Checklist.

Training. Provide all training and user guidance needed to ensure appropriate system use, data entry, data reporting, and data security and confidentiality.

Helpdesk support. Receives, triages, and resolves technical issues in the AKHMIS experienced by the users.

Data analysis and reporting. Analyzes data for the two AK CoCs, including non-HMIS data. Interprets, visualizes, and presents data to the AK CoCs. Ensures the AK CoCs reporting requirements are met.

Communications. Disseminates information to the community and manages communications related to data on behalf of the AK CoCs.

REFERENCES

- AKHMIS Governance Charter [External link]
- AKHMIS Data Quality Plan [External link]
- HMIS Data Standards [External link]
- CoC Program HMIS Manual [External link]
- ESG Program HMIS Manual [External link]
- YHDP HMIS Manual [External link]
- PATH Program HMIS Manual [External link]
- HOPWA Program HMIS Manual [External link]
- HUD-VASH Program HMIS Manual [External link]
- VA Programs HMIS Manual [External link]
- RHY Program HMIS Manual [External link]
- HMIS System Administrator Checklist [External link]

6.1 CHO PROJECT NAMING CONVENTION

POLICY

All projects in the AKHMIS will be named with the following information: the organization (CHO) operating the project, the project's name so that it is easily identified by users at the organization that will be entering data, and the project's type to reflect the type of service to be provided by the project.

PROCEDURE

All projects will include the AKHMIS-participating organization name, project name, project type and a unique project identifier.

REFERENCES

- HMIS Data Standards [External link]
- CoC Program HMIS Manual [External link]
- ESG Program HMIS Manual [External link]
- YHDP HMIS Manual [External link]
- PATH Program HMIS Manual [External link]
- HOPWA Program HMIS Manual [External link]
- HUD-VASH Program HMIS Manual [External link]
- VA Programs HMIS Manual [External link]
- RHY Program HMIS Manual [External link]

6.2 COVERED HOMELESS ORGANIZATION (CHO) RESPONSIBILITIES

POLICY

Covered Homeless Organizations are required to meet the responsibilities agreed to when signing AKHMIS related participation agreement documents.

PROCEDURE

The CHOs – including AKHMIS users within the CHO – are responsible for following AKHMIS requirements detailed in the following:

- AKHMIS Policies and Procedures Manual
- Various AKHMIS Participation Agreement documents
- AK CoC Statewide Privacy Policy
- AK CoC Statewide Security Policy
- AK CoC Statewide Consumer Notice
- AKHMIS User Agreement
- AKHMIS Data Quality Plan

AKHMIS-participating organization responsibilities include, but are not limited to:

- Ensure the CHO obtains a unique user license for each AKHMIS user at the organization.
- Establish the standard reports for each specific project created.
- Ensure a minimum standard of data quality by accurately answering the Universal Data Elements and required program-specific data elements for every individual entered into the AKHMIS.
- Ensure AKHMIS-participating organization staff receive required AKHMIS training, and review the AKHMIS Policies and Procedures, Alaska Continuums of Care (AK CoCs) Privacy Policy, Alaska Continuums of Care (AK CoCs) Security Policy, AKHMIS Data Quality Plan and any other AKHMIS-related documents.
- Ensures that the projects are in compliance with the standards set in the AKHMIS Data Quality Plan.
- Ensure that AKHMIS access is granted only to staff members who have received training, have completed the AKHMIS User Agreement, and are authorized to use the AKHMIS.
- Notify all users at their organization of interruptions in service.
- The AKHMIS-participating organization shall ensure that all staff and volunteers issued a User ID and password for HMIS will read the AKHMIS email newsletter.
- Administer and monitor data security policies and standards, including:
  - User access control
  - Backup and recovery of data
  - Detection and response to violations of the policies and procedures or Organization procedures

REFERENCES

- AKHMIS Data Quality Plan Participating Organization Agreement [External link]
- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]
- AKHMIS Coordinated Services Agreement [External link]
- Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements [External link]
- Participation Agreement Documents [AKHMIS Policy: Internal link]

6.3 PARTICIPATION AGREEMENT DOCUMENTS

POLICY

Covered Homeless Organizations will sign AKHMIS related participation agreements within ten business days of receiving the documents.

PROCEDURE

CHOs must complete and sign AKHMIS related documents and agreements, including but not limited to the following:

AKHMIS Organization Partnership Agreement: Must be signed by each CHO's Executive Director on an annual basis. ICA will retain theoriginal document. The AKHMIS Organization Partnership Agreement states the Organization's commitment to adhere to the policies and procedures for effective use of the AKHMIS.

AKHMIS User Agreement: Details user policies and responsibilitiesand is signed by each authorized user, then renewed annually. Signed copies of these must be sent to ICA. An electronic or hard copy of the original document must be kept by the originating Organization.

AKHMIS Coordinated Services Agreement: Allows the specifically named AKHMIS user toenter client data as, or on behalf of, another specifically named CHO and / or to report on behalf of the specifically named CHO. The signed agreement will be maintained byICA.

Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements: Must be signed by the Executive Directorof each CHO participating in data sharing related to the AKHMIS. ICA will retain the original document.

AKHMIS Data Quality Plan Participating Organization: All organizations participating in AKHMIS will be required to sign a AKHMIS Data Quality Plan Organization Agreement for access to HMIS. Must be signed by each CHO's Executive Director on an annual basis. This Agreement will require the organization to participate in and abide by the processes and standards provided within this document.

REFERENCES

- AKHMIS Data Quality Plan Participating Organization Agreement [External link]
- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]
- AKHMIS Coordinated Services Agreement [External link]
- Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements [External link]
- AKHMIS Operating Policies Violation [AKHMIS Policy: Internal link]

6.4 ALASKA COC STATEWIDE INTERORGANIZATIONAL DATA SHARING PARTICIPATING COVERED HOMELESS ORGANIZATIONS (CHOS)

POLICY

A list of organizations who have signed an Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements will be maintained.

PROCEDURE

ICA maintain the list of organizations who have signed an Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements.

A copy of the list will be available on the ICA website.

REFERENCES

- Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements [External link]
- Participation Agreement Documents [AKHMIS Policy: Internal link]

6.5 HMIS USER LICENSES

POLICY

CHOs may request AKHMIS user licenses for staff, contract workers, or volunteers within the CHO at any time.

PROCEDURE

ICA/AK CoCs. License fees are paid for by HUD CoC and AHFC funding. The AK CoCs reserve the right to change the license acquisition and allocation process based upon funding availability.

The ART license is an add-on license available for AKHMIS users to facilitate data reporting. The cost of an ART license will be paid for by funding from the HUD CoC and AHFC grants. The AK CoCs reserve the right to change the ART license acquisition, allocation, and associated costs.

If additional AKHMIS licenses need to be purchased, ICA will obtain approval from the AK CoCs prior to purchase.

Supervisors. Supervisors are required to request the AKHMIS User License and the ART License for their staff via the AKHMIS Help Desk.Supervisors are required to advise ICA when a user no longer needs a license within 24 hours of when a user no longer needs to access the AKHMIS.

AKHMIS Users. AKHMIS Users responsibilities include, but are not limited to:

- Sign the AKHMIS User Agreement and complete required AKHMIS training.
- Take appropriate measures to prevent unauthorized data disclosure.
- Report any security violations in accordance with the AK CoCs Security Plan.
- Comply with relevant policies and procedures.
- Input required data fields in a consistent, accurate, and timely manner.
- Ensure a minimum standard of data quality as defined by the Data Quality Plan.
- Inform clients about the Organization’s use of the AKHMIS.
- Take responsibility for any actions undertaken with one’s AKHMIS username and password.
- Read the AKHMIS Newsletter from ICA.
- Respond to requests from ICA in a timely manner.
- **Never** access areas of AKHMIS on which they were not trained by an ICA staff member.

REFERENCES

- AKHMIS Governance Charter [External link]
- AKHMIS Data Quality Plan [External link]
- AKHMIS Data Quality Plan Participating Organization Agreement [External link]
- AKHMIS User Agreement [External link]

6.6 USER CONFLICT OF INTEREST

POLICY

Users who are also clients with records in the AKHMIS are prohibited from entering or editing information in their own record. All users are also prohibited from entering or editing information in records of immediate family members.

PROCEDURE

All users must sign the AKHMIS User Agreement, which includes a statement describing this limitation, and report any potential conflict of interest to their Program Director or Executive Director. ICA may run the audit trail report to determine if there has been a violation of the conflict of interest agreement.

REFERENCES

- Client Confidentiality [AKHMIS Policy: Internal link]

6.7 CLIENT CONFIDENTIALITY

POLICY

AKHMIS users will comply with all policies and procedures related to maintaining client privacy and protecting client information.

PROCEDURE

The AKHMIS user will sign an annual AKHMIS User Agreement regarding the allowable uses of their AKHMIS user name and password, and the user's intention to comply with all policies and procedures governing the use of the AKHMIS and the data therein.

The confidentiality agreement will include, but is not limited to the following:

- The user has read and understands the Alaska CoC Statewide Privacy Policy and is aware of the allowable uses and disclosures of clients' Personally Identifiable Information (PII).
- The user will ensure that the Alaska CoC Statewide Privacy Policy is explained to clients during the intake process and will make the Alaska CoC Statewide Privacy Policy available to clients upon request.
- The user understands that their AKHMIS user name and password must not be shared with anyone, including other staff or volunteers within their Organization. The user will take all reasonable means to keep their AKHMIS username and password physically secure.
- The user may only view, obtain, disclose, search for, or use the database information that is necessary to perform the official duties of their job.
- The user will log out of AKHMIS each time they must leave the work area where the computer is located.
- The user will attend any AKHMIS and related topic training sessions, as required, to ensure accurate and appropriate data entry and use of the AKHMIS.
- The user will ensure that any computer used to access the AKHMIS is located in an area that can be physically secured with a lock when not in use by the authorized staff person.
- The user will never leave any computer unattended that has the AKHMIS "open and running."
- The user will ensure that any computer used to access the AKHMIS is equipped with a password protected screensaver.
- The user would report to their organization according to their internal Policies and Procedures if a computer used for AKHMIS access does not have required virus protection software with auto update functions and/or hardware firewall protection installed on the computer. If no action is taken by the Organization, the user will contact ICA.
- The user understands that failure to log out of the AKHMIS appropriately may result in a breach in client confidentiality and system security, and that this is considered a violation of the Alaska CoC Statewide Privacy Policy and the Alaska CoC Statewide Security Policy.
- The user will follow their organization's policies regarding the secure storage of hard copies of AKHMIS information.
- The user will properly destroy hard copies of AKHMIS information when it is no longer needed to maintain confidentiality, according to their organization's internal policies regarding the destruction of hard copies of AKHMIS information.
- If the user witnesses or suspects a security breach, they or their organization will immediately send written notification of the issue to the applicable CoC and ICA.
- If the user has a conflict of interest in entering data into the AKHMIS, they will disclose that to their Program Director. If the user is a client within the AKHMIS, or has immediate family members within the AKHMIS, they will not access or make changes to those records in the AKHMIS.

All users are required to sign the Confidentiality Agreement portion of the annual User Agreement acknowledging that they will maintain confidentiality about any information they become aware of regarding any client in AKHMIS. Violations of the Confidentiality Agreement include, but are not limited to:

- Attempting to access confidential information without specific authorization.
- Taking photographs of AKHMIS information without specific authorization.
- Telling another person about any client-related information they have become aware of while accessing the AKHMIS.
- Intentional or negligent mishandling or destruction of confidential information.
- Leaving a secured computer application unattended while signed into the AKHMIS.
- Attempting to access a secured computer application or restricted area without proper authorization or for purposes other than official AKHMIS business.

Any violation of the Confidentiality Agreement may result in termination of the user's access to AKHMIS.

REFERENCES

- User Conflict of Interest [AKHMIS Policy: Internal link]
- Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

6.8 TRAINING PROGRAM

POLICY

The ICA will develop and maintain a training program and resources to provide to users that will facilitate high levels of data completeness and data quality. ICA will maintain and update the training program and resources to reflect current HMIS data standards and will ensure availability of the training program and resources to all users.

PROCEDURE

ICA must offer training sessions at reasonable intervals.

Training on data entry will be conducted using training programs that are separate from AKHMIS data and are never included in any AKHMIS reports.

ICA staff offers standard, regularly scheduled training at no cost to users at CHOs.

6.9 USER TRAINING

POLICY

All new AKHMIS users are required to successfully complete the AKHMIS new user training process with ICA prior to receiving access to the system.

If ICA determines that data entered by a current user does not meet minimum data quality standards, ICA reserves the right to require users to complete refresher training(s).

Covered Homeless Organization (CHO) HMIS Data Entry Training. User data entry requests for specific projects within an organization must be completed by supervisors within the organization via the Training Request Form on the ICA Alaska website. Submissions are received by ICA in the AKHMIS Help Desk.

Coordinated Entry (CE) HMIS Data Entry Training. Coordinated Entry data entry training requests must be submitted by the local coalition via the Coordinated Entry certification form on the ICA Alaska website. Submissions are received by ICA in the AKHMIS Help Desk.

It is mandatory that users be trained by the local coalition on their local CE System and CE Policies prior to submitting a CE data entry training request to ICA.

PROCEDURE

Unless otherwise specified, workflow and group trainings occur via GoToMeeting or other similar software.

Supervisors and/or local Coalitions must ensure that AKHMIS trainees have received training on AKHMIS responsibilities by their organization prior to submitting an AKHMIS data entry training request, or by the local coalition on their local CE System and CE Policies prior to submitting a CE data entry training request. These responsibilities include:

- Understanding of the AKHMIS project(s) the trainee will access.
- How the organization collects client data (i.e. on paper documents, entered in live time into the AKHMIS, collected by an intake worker that is then entered into the HMIS by someone else).
- Trainee's role for data entry.
- Project's eligibility criteria for clients.

If a user does not have an understanding of the procedures that require the requested HMIS workflow training, the AKHMIS training may be postponed.

New User Training Requirements. Trainees must complete initial training steps within 20 business days of the training request submission. Upon completion of the initial training steps, the trainee will choose a date on the ICA training calendar on which they would like to complete their workflow-specific training. The workflow-specific training must be scheduled within one month of completion of the initial training steps. If these initial steps are not completed within the specified time period, trainees may be required to retake the initial training steps.

If a trainee needs to be trained on more than one workflow, each workflow will generally have a separate training.

After a trainee completes the workflow-specific training, the trainee has five business days to submit the corresponding required practice case(s) into the AKHMIS Training Site. ICA staff will review practice cases and determine if corrections are needed. Trainees will have an additional five business days to complete corrections. If the trainee does not complete all requirements within 20 days of the start of their workflow-specific AKHMIS training and still needs access to the AKHMIS, the trainee will be administered a practice case to enter into the AKHMIS Training Site. If there are corrections needed, the trainee will be required to redo all or some of the training process based on ICA’s discretion.

ICA staff may determine that a trainee did not retain the necessary data entry concepts based on the quality of the trainee's practice case submission(s) into the AKHMIS Training Site. ICA staff may use their discretion to require trainees to complete additional training sessions with ICA until the trainee meets the required standard of data entry in order to gain access to the AKHMIS. If a trainee is unable to successfully complete all assignments for data entry after repeated attempts, ICA staff may use their discretion to determine that the trainee is not capable of accurate and complete data entry and may deny access to the AKHMIS.

Trainees may request permission from ICA to take the new user training series over a longer period if a trainee is unable to attend training with ICA within the period of time allowed. ICA must receive the request in writing prior to the start of the new user training series.

New Organization/Existing User Training Requirements. If a trainee has previously had an AKHMIS user license, the trainee will be required to complete necessary training steps identified by ICA staff in order to access the AKHMIS. ICA has sole discretion to waive the requirement to attend new user training. ICA will consider a trainee's familiarity with the AKHMIS and the need for the trainee to learn about system updates and changes when making a decision to waive the new user training requirement.

REFERENCES

- Covered Homeless Organization (CHO) Responsibilities [AKHMIS Policy: Internal link]
- AKHMIS Data Quality Plan [External link]

6.10 USER REQUIREMENTS FOR MAINTAINING USER LICENSE

POLICY

On an annual basis, all AKHMIS users are expected to sign the AKHMIS User Agreement and complete the AKHMIS Privacy and Security Training module. The Privacy and Security Training module covers HMIS security and privacy measures outlined in HUD's Federal Register HMIS Data and Technical Standards Final Notice. The Annual User Requirements must include a Privacy and Security Training review and must be made available to all users at all CHOs, and include execution of a new AKHMIS User Agreement with a deadline for completion.

PROCEDURE

ICA will:

- Provide all information to users pertaining to Annual User Requirements via the AKHMIS Listserv (dates/times, links to training, documents, reminders, and deadlines).
- ICA will send reminders for the Annual User Requirements completion deadline via the AKHMIS Listserv.

All users are required to complete the Privacy and Security Training annually, including passing the associated knowledge-based quiz.

User activity. ICA will run a report once a month on user activity. If a data entry user has not logged into AKHMIS within the 45 days prior to the report run date, ICA will contact the contact person at the user's organization to confirm their access need. If a response is received that the user still needs access, the user may need to complete an AKHMIS practice case in the AKHMIS training site to ensure that the user is able to maintain acceptable data quality. ICA may provide additional training to the user. If a response is received that the user is no longer an active participant in AKHMIS data entry, ICA will remove their access to HMIS. If no response is received within five days, the user's license will be expired.

REFERENCES

- AKHMIS User Agreement [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]
- Covered Homeless Organization (CHO) Responsibilities [AKHMIS Policy: Internal link]
- HUD Federal Register HMIS Data and Technical Standards Final Notice [External link]

6.11 UNEXCUSED TRAINING ABSENCE

POLICY

Trainees registered for a scheduled training session with ICA are expected to attend or properly notify ICA if they need to cancel or reschedule a training session.

> ***Please note**: This policy applies to scheduled training sessions with an ICA trainer. It does not apply to self-administered online video training.*

PROCEDURE

A trainee’s unexcused absence from workflow-specific trainings with an ICA trainer takes away time available for training other users. If a trainee misses a scheduled workflow-specific training, it is the trainee’s responsibility to reschedule their training. If the rescheduled training is not completed within one month of completion of the initial training steps, trainees may be required to retake the initial training steps.

After two consecutive unexcused training absences, the trainee’s supervisor will need to meet with ICA to set another training time for the trainee.

After three unexcused training absences, the CoC will be notified by ICA to determine what action should be taken.

EXEMPTIONS

Exemptions to this policy may be granted by an AKHMIS System Administrator.

REFERENCES

- AKHMIS User Agreement [External link]

7 VENDOR SUPPORT AND PERFORMANCE

POLICY

Technical Performance. The vendor maintains the system, including data backup, data retrieval, and server functionality / operation. Upgrades to the system software will be continuously developed and implemented.

Technical Support. The vendor will assist ICA to resolve software problems, make necessary modifications for special programming, and will explain system functionality to ICA.

PROCEDURE

The requirements of AKHMIS software vendor WellSky^{TM} are specified in the contract for AKHMIS vendor services, including the requirements specified in this policy.

8 MINIMUM TECHNICAL STANDARDS

POLICY

AKHMIS Users must ensure their equipment meets the minimum requirements described herein.

PROCEDURE

Minimum Computer Requirements:

- A PC with a 2 Gigahertz or higher processor, 40GB hard drive, 512 MB RAM, and Microsoft Windows 7 or 8.
- The most recent version of Google Chrome, Safari, Microsoft Edge, or Firefox. No additional plug-in is required.
- It is recommended that your browser have a 128 cipher / encryption strength installed. The browser's cache should be set to "Check for new version of the stored pages: Every visit to page."
- A broadband Internet connection or LAN connection. Dial-up modem connections are not sufficient.
- Virus protection updates.
- The only mobile device that is officially supported by Mediware Information Systems is the Apple iPad running the latest version of iOS.

Additional Recommendations:

- A Dual-Core processor is recommended
- 1024x768 (XGA) or higher monitor/screen display; 1280x768 strongly advised

REFERENCES

- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]
- Health Insurance Portability and Accountability Act (HIPAA) regulations [External link]
- 2004 HMIS Data and Technical Standards Final Notice [External link]

8.1 AKHMIS OPERATING POLICIES VIOLATION

POLICY

AKHMIS users and CHOs must abide by all AKHMIS operational policies and procedures outlined herein, the AKHMIS User Agreement, Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements, and the AKHMIS Organization Partnership Agreement. Repercussions for any violation will be assessed in a tiered manner. Each user or CHO violation will face successive consequences – the violations do not need to be of the same type to be considered second or third violations. AKHMIS user violations do not expire. No regard is given to the duration of time that occurs between successive violations of the AKHMIS operational policies and procedures as it relates to corrective action.

PROCEDURE

First violation. The user and CHO will be notified of the violation in writing by ICA. The user's license will be suspended for 30 days, or until the CHO notifies ICA of action taken to remedy the violation. ICA will provide necessary training to the user and / or CHO to ensure the violation does not continue. ICA will notify the Executive Directors of the AK CoCs of the violation.

Second violation. The user and CHO will be notified of the violation in writing by ICA. The user's AKHMIS license will be suspended for 30 days. The user and / or CHO must take action to remedy the violation; however, this action will not shorten the length of the license suspension. If the violation has not been remedied by the end of the 30-day user license suspension, the suspension will continue until the CHO notifies ICA of the action taken to remedy the violation. ICA will provide necessary training to the user and / or CHO to ensure the violation does not continue. ICA will notify the Executive Directors of the AK CoCs of the violation.

Third violation. The user and CHO will be notified of the violation in writing by ICA. ICA will notify the Executive Directors of the AK CoCs of the violation who will determine if the user's license should be terminated. The user's license will be suspended for a minimum of 30 days, or until the AKHMIS CoC notifies ICA of their determination, whichever occurs later. If the AK CoC determines the user should retain their user license, ICA will provide necessary training to the user and / or CHO to ensure the violation does not continue. If users who retain their license after their third violation have an additional violation, that violation will be reviewed by the CoC.

NOTIFYING ICA OF A VIOLATION

It is the responsibility of the Executive Director, Program Director, or general User to notify ICA when they suspect that a User or CHO has violated any AKHMIS operational agreement, policy, or procedure. A complaint about a potential violation must include the User and CHO name, anda description of the violation, including the date or timeframe of the suspected violation. Complaints should be sent in writing to ICA at AKHMIS@icalliances.org. The name of the person making the complaint will not be released from ICA if the individual wishes to remain anonymous.

VIOLATIONS OF LOCAL, STATE, OR FEDERAL LAW

Any CHO or user in violation of local, state, or federal law will immediately be subject to the consequences listed under the Third Violation above.

MULTIPLE VIOLATIONS WITHIN A 12-MONTH TIMEFRAME

During a 12-month calendar year, if there are multiple users (3 or more) with multiple violations (2 or more) from one CHO, the CHO as a whole will be subject to the consequences listed under the Third Violation above.

EGREGIOUS VIOLATIONS

Additionally, although violations will typically result in progressive consequences, the actual consequence depends on the seriousness of the violation, which could include termination of access rights as the first step, as determined at the discretion of ICA in consultation with the AK CoCs' Executive Committees.

APPEALS PROCESS

Any CHO or user whose access to AKHMIS has been suspended or revoke has the right to submit a written appeal request to the AK CoC, the AKHMIS Advisory Board and ICA. The AK CoC will convene a review panel made up of the AKHMIS Advisory Board members who will determine if the user's license should be terminated. The decision of the panel will be submitted in writing to the AK CoC within 30 of receipt of the appeal request.

REFERENCES

- AKHMIS User Agreement [External link]
- AKHMIS Organization Partnership Agreement [External link]
- AKHMIS Coordinated Services Agreement [External link]
- Alaska CoC Statewide Interorganizational Data Sharing and Coordinated Services Agreements [External link]
- Participation Agreement Documents [AKHMIS Policy: Internal link]

9 GLOSSARY

Alaska Continuums of Care Statewide Privacy Policy (AK CoC Statewide Privacy Policy): The Policy that governs allowable uses and disclosures of personally identifiable information for the purposes of AKHMIS and / or the Coordinated Entry System.

Alaska Continuums of Care Statewide Security Policy (AK CoC Statewide Security Policy): The Policy that governs how equipment used to access AKHMIS and / or the Coordinated Entry System must be protected from misuse, a breach, or a violation of personally identifiable information.

Alaska Homeless Management Information System (AKHMIS): An internet-based database that is used by covered homeless organizations across the State of Alaska to record and store client-level information about the numbers, characteristics, and needs of persons at-risk of or experiencing homelessness.

Alaska Homeless Management Information System Advisory Board (AKHMIS Advisory Board): The advisory board is responsible for monitoring the performance of the AKHMIS. As part of this responsibility, the board is tasked with working in conjunction with the ICA Agency to make recommendations on improvements to the AKHMIS, which are then provided to the Executive Committees of the AK CoCs for approval and implementation.

Closed Data: Information entered into the AKHMIS by one Covered Homeless Organization that is not visible to other Covered Homeless Organizations accessing the AKHMIS.

Confidential Data: Information that contains personally identifiable information.

Covered Homeless Organization (CHO): Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, or processes PII on clients at-risk of or experiencing homelessness for an HMIS. This definition includes both organizations that have direct access to the AKHMIS, as well as those organizations who do not but do record, use, or process PII.

User: An individual at a Covered Homeless Organization who has a user license to enter data into the AKHMIS.

Institute for Community Alliances (ICA): Organization that serves as the HMIS Lead Agency for the State of Alaska.

HMIS Solution Provider (aka Vendor): The AKHMIS solution provider (vendor) is WellSky^{TM}. The HMIS vendor designs the HMIS and provides ongoing support to the HMIS Lead Agency.

Minimum Data Entry Standards: A mandatory set of data elements that must be collected and entered into the AKHMIS for each client served by projects. These standards include both the Universal Data Elements (UDEs) and the Program-Specific Data Elements (PSDEs).

Open Data: Does not include personally identifiable information.

Open Public Data: Aggregate data only, with no client-level information. Data cannot be traced back to any client.

Open Restricted Data: De-identified data (PII has been removed) with multiple elements of information available per client. Data cannot be traced back to any client.

Personally Identifiable Information (PII): Any information maintained by or for a CHO about a client at-risk of or experiencing homelessness that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Program: Refers to the federal funding stream used to provide dollars to specific projects operating to serve clients at-risk of or experiencing homelessness.

Program Director: An individual at a Covered Homeless Organization whose title is Program Director, Executive Director, or comparable title.

Project: Refers to a distinct unit of an organization, which may or may not be funded by HUD or the federal partners, that provides services and / or shelter / housing for individuals at-risk of or experiencing homelessness and is identified by the AK CoCs as part of their service system.

Shared Data: Unrestricted information that has been entered by one Covered Homeless Organization and is visible to other Partner Organizations using the AKHMIS. Shared data can also include data that is disclosed from the AKHMIS for the purposes laid out in the AK CoC Statewide Privacy Policy.