Kansas Statewide Homeless Coalition

Kansas Balance of State Continuum of Care Homeless Management Information System Policies and Procedures

KANSAS HOUSING

Contents

PROJECT SUMMARY

Introduction

A Homeless Management Information System (HMIS) is a database used to record and track client-level information on the characteristics and service needs of homeless persons. An HMIS ties together homeless service providers within a community to help create a more coordinated and effective housing and service delivery system.

The U. S. Department of Housing and Urban Development (HUD) and other planners and policymakers at the federal, state, and local levels use aggregate HMIS data to obtain better information about the extent and nature of homelessness over time. Specifically, an HMIS can be used to produce an unduplicated count of homeless persons, understand patterns of service use, and measure the effectiveness of homeless programs.

Kansas Balance of State HMIS is staffed at the Kansas Statewide Homeless Coalition, Kansas Housing Resource Corporation and COC HMIS Committee. Kansas Housing Resource Corporation has been designated by the COC as the Lead Agency to operate the HMIS to ensure high data quality and other HUD HMIS compliance of all HUD/ESG/COC/PATH Program Projects and other projects required to use HMIS in the KS BOS COC. Kansas Housing Resource Corporation performs these tasks at the direction of the COC, through the KS BOS COC Board.

Agencies that participate in Kansas Balance of State's HMIS are referred to as "participating agencies." Each participating agency needs to follow certain guidelines to help maintain data privacy and accuracy. The guidelines listed in this document do not replace the more formal and legally binding agency agreement that each agency signs before program implementation.

History

In 2001, Congress instructed the U.S. Department of Housing and Urban Development (HUD) to take measures to improve available data concerning homelessness in the United States. In response, HUD mandated all Continuums of Care regions to implement region-wide databases that would allow an unduplicated count of clients served. Out of this directive came the Homeless Management Information System (HMIS), a computerized data collection application that facilitates the collection of information on homeless individuals and families using residential or other homeless assistance service agencies, and stores that data in a centralized database for analysis.

Why is this important?

Having access to the HMIS represents a strategic advantage for service providers. The HMIS software selected by the Kansas Balance of State COC allows multi-level client data sharing between organizations, as well as client case coordination and electronic referrals. Our locally developed information-sharing model can prevent service duplications and enable collaboration between various homeless service providers, while limiting access to sensitive data. Client privacy is very important to us. In addition to the standard data collection and reporting functionalities, the HMIS software includes a comprehensive case management module, bed management, performance measurement tools, ad-hoc reporting, software customization options, etc.
Lastly, providers already in HMIS are better positioned to apply for future funding opportunities, as many national and local funders now require HMIS participation

ROLES AND RESPONSIBILITIES

Kansas Balance of State COC HMIS Responsibilities

- Execute HMIS participation agreements;
- Monitor participating agencies compliance with applicable HMIS standards on a regular basis;
- Establish and review annually End User Agreements;
- Ensure maintenance and updates as needed the files for HMIS software to include software agreements, HUD Technical Submissions, HUD executed agreements, APR, and CAPER;
- Develop and maintain HMIS agency files to include original signed participation agreements, original signed user license agreements and all other original signed agreements pertaining to HMIS;
- Develop and update as needed a Data Quality Plan;
- Review and update HMIS Privacy Policy yearly;
- Develop and review annually the HMIS Security Plan, including disaster planning and recovery strategy;
    - Review and update as need HMIS Policies and Procedures;
    - Provide copies of the Data Quality Plan, Privacy Policy, Security Plan and Policy and Procedures to the HMIS Committees for review and feedback on an annual basis or PRN.
    - Review national, state, and local laws that govern privacy or confidential protections and make determinations regarding relevancy to existing HMIS policy;
    - Provide new user training and refresher user training yearly or PRN;
    - Pro-actively contact new users for immediate follow up and issuance of username and password to access HMIS to begin entry of data as soon as possible following training;
    - Provide on-site technical support to agencies using HMIS for troubleshooting and data input;
    - Monthly review of HMIS data and bed lists to ensure that participating agency programs are using HMIS accurately;
    - Provide assistance to agencies upon request for additional on-site training and support
    - Conduct unduplicated accounting of homelessness annually.

Participating Agency Responsibilities

- Must comply with all applicable agreements;
- Execute and manage HMIS User License Agreements with all staff who have HMIS access;
- Comply with the HMIS Standards and Policies as appropriate;
- Accurately enter all required data into the HMIS system, including accurate and timely information into housing, where applicable.

IMPLEMENTATION POLICIES AND PROCEDURES

HMIS Agency Participation Agreement

The Executive Director of any Participating Agency shall follow, comply, and enforce the HMIS Agency Participation Agreement (Appendix A). The Executive Director must sign an HMIS Agency Participation Agreement before granted access to HMIS. Signing of the HMIS Agency Participation Agreement is a precursor to training and user access.

- An original signed HMIS Agency Participation Agreement must be presented to the HMIS staff before any program is implemented in the HMIS.
- After the HMIS Agency Participation Agreement is signed, the HMIS staff will train end users to use HMIS.

- A username and password will be granted to end users after required training is completed.

HMIS User License Agreement

End user of any Participating Agency shall follow, comply, and enforce the HMIS User License Agreement (Appendix B). Before given access to HMIS, the end user must sign an HMIS User License Agreement.

- The HMIS staff will provide the end user a HMIS User License Agreement for signature after completing required training.
- The HMIS staff will collect and maintain HMIS User License Agreements of all end users.

Data Collection Requirements

Participating Agencies will collect and verify the minimum set of data elements for all clients served by their programs within the timeframe outlined in the HMIS Data Quality Plan (Appendix C).

- During client intake, end users must collect all the universal data elements set forth in the most recent version of the HMIS Data Standards Manual located on HUD Exchange at https://www.hudexchange.info/resource/3824/hmis-data-dictionary/. The universal data elements may include:
    - o Name
    - o Social Security Number
    - o Date of Birth
    - o Race
    - o Ethnicity
    - o Gender
    - o Veteran Status
    - o Disabling Condition
    - o Residence Prior to Project Entry
    - o Project Entry Date
    - o Project Exit Date
    - o Destination
    - o Relationship to Head of Household
    - o Client Location
    - o Length of Time on Street, in an ES or Safe Haven

- End users must also collect all the program-specific data elements at program entry and exit set for in the most recent version of the HMIS Data Standards Manual. The program-specific data elements include:
    - o Housing Status
    - o Income and Sources
    - o Non-Cash Benefits
    - o Health Insurance
    - o Physical Disability
    - o Developmental Disability
    - o Chronic Health Condition
    - o HIV/AIDS
    - o Mental Health Problem
    - o Substance Abuse
    - o Domestic Violence
    - o Contact
    - o Date of Engagement
    - o Services Provided
    - o Financial Assistance Provided
    - o Referrals Provided
    - o Residential Move-In Date
    - o Housing Assessment Disposition
    - o Housing Assessment at Exit

HMIS Program Entry and Exit Date

End users of any Participating Agency must record the Program Entry Date of a client into HMIS no later than three (3) business days upon entering the program.

End Users of any Participating Agency must record the Program Exit Date of a client into HMIS no later than three (3) business days after exiting the program or receiving their last service.

- End user must enter the month, day, and year of program enrollment and program exit.

- For returning clients, end user must record a new Program Entry Date and corresponding Program Exit Date.
- The system will trigger a warning when end users enter a Program Exit Date that is earlier than the Program Entry Date for a client.

HMIS Technical Support Protocol

The HMIS staff will provide a reasonable level of support to Participating Agencies via email, phone, and/or remote.

1. HMIS Users should first seek technical support from their agency HMIS expert.
2. If more expertise is required to further troubleshoot the issue, agency HMIS expert or HMIS User should submit request to:
    a. HMIS Support for general technical support at hmis@kshomeless.com. Refrain from sending email correspondence directly to the HMIS Support Team.
3. Technical Support Hours are Monday through Friday (excluding holidays) from 8:00 AM to 5:00 PM.
4. Provide issue replication details if possible (or help recreate the problem by providing all information, screenshots, reports, etc.) so HMIS staff can recreate problem if required.
5. The HMIS staff will try to respond to all email inquiries and issues within three (3) business days, but support load, holidays, and other events may affect response time.
6. The HMIS staff will submit a ticket to software vendor if progress is stalled.

Participation Fees

The Kansas Balance of State COC reserves the right to charge a participation fee to use the system. Refer to the HMIS Fee Schedule (Appendix D) regarding fees.

SECURITY POLICIES AND PROCEDURES

Training

Each end user must complete the required New User Training prior to gaining access to HMIS. HMIS staff will provide training to all end users

- HMIS staff will provide New User Training to proposed end users.
- HMIS staff will provide new end users with a copy of the HMIS Policies and Procedures and HMIS User Guide.
- The table below lists the training courses offered.

Course Description	Course Detail
New User Training	Users will learn the basic skills and concepts needed to complete client intake process
User Refresher Training	Help to refresh the skills of active users, as well as review any issues users may have with navigating through the system or the data collection process
Reports Training	Users are given and overview of the various reporting options available in the HMIS
Data Explorer	Trains experienced users, with good knowledge of the existing HMIS reports, on the usage of the HMIS ad hoc data analysis tools.

User Authentication
Only users with a valid username and password combination can access HMIS. The HMIS staff will provide unique username and initial password for eligible individuals after completion of required training and signing of the HMIS User License Agreement.

- The Participating Agency will determine which of their employees will have access to the HMIS. User access will be granted only to those individuals whose job functions require legitimate access to the system.
- Proposed end user must complete the required training and demonstrate proficiency in use of system.
- Proposed end user must sign the HMIS User License Agreement stating that he or she has received training, will abide by the Policies and Procedures, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in the system relevant to the delivery of services to people.
- The HMIS staff will be responsible for the distribution, collection, and storage of the signed HMIS User License Agreements.
- The HMIS staff will assign new users with a username and an initial password.
- Sharing of usernames and passwords is a breach of the HMIS User License Agreement since it compromises the security to clients.
- The Participating Agency is required to notify the HMIS staff when end user leaves employment with the agency or no longer needs access as soon as possible following the end user leaving the agency.
- Users not logging into HMIS for more than 45 days will be locked out due to non-activity.

Passwords
Each end user will have access to HMIS via a username and password. Passwords will be reset every 180 days. End users will maintain passwords confidential.

- The HMIS staff will provide new end users a unique username and temporary password after required training is completed.
- End user will be required to create a permanent password that is between eight and sixteen characters in length. It must also contain characters from the following four categories: (1) uppercase characters (A through Z), (2) lower case characters (a through z), (3) numbers (0 through 9), and (4) non-alphabetic characters (for example, $, #, %).
- End users may not use the same password consecutively but may use the same password more than once.
- Access permission will be revoked after the end user unsuccessfully attempts to log on five times. The end user will be unable to gain access until the HMIS staff reset their password.

Hardware Security Measures
All computers and networks used to access HMIS must have virus protection software and firewall installed. Virus definitions and firewall must be regularly updated.

Security Review
HMIS staff will complete an annual security review to ensure the implementation of the security requirements for itself and Participating Agencies. The security review will include the completion of a security checklist ensuring that each security standard is implemented. The KS BOS COC board has selected the HMIS Governance Committee to serve as the Security Officers.

Security Violations and Sanctions

Any end user/agency found to be in violation of security protocols of their agency's procedures or HMIS Policies and Procedures will be sanctioned accordingly. All end users/agencies must report potential violation of any security protocols.

- End users are obligated to report suspected instances of noncompliance and/or security violations to their agency and/or HMIS staff as soon as possible.
- The Participating Agency or HMIS staff will investigate potential violations.
- Any end user/agency found to be in violation of security protocols will be sanctioned accordingly. Sanction may include but are not limited to suspension of system privileges and revocation of system privileges.

CLIENT INFORMED CONSENT AND PRIVACY RIGHTS

Participating Agencies must obtain informed consent prior to entering any client personal identifiable information into HMIS. Written consent is required for data sharing. Services will not be denied if a client chooses not to include personal information. Personal information collected about the client should be protected. Each Participating Agency and end user must abide by the terms in the HMIS Agency Participation Agreement (Appendix A) and HMIS User License Agreement (Appendix B).

- Client must sign the Authorization to Disclose Client Information form (Appendix E) or consent of the individual for data collection may be inferred from the circumstances of the collection. Participating Agencies may use the Inferred Consent Notice (Appendix F) to meet this standard.

- Clients that provide permission to enter personal information allow for Participating Agencies within the continuum to share client and household data.
- If client refuses consent, the end user should not include any personal identifiers (First Name, Last Name, Social Security Number, and Date of Birth) in the client record.
- For clients with consent refused, end user should include a client identifier to recognize the record in the system.
- Participating Agencies shall uphold Federal and State Confidentiality regulations and laws that protect client records.

The HMIS standards and the HIPAA standards are mutually exclusive. An organization that is covered under the HIPAA standards is not required to comply with the HMIS privacy or security standards, so long as the organization determines that a substantial portion of its protected information about homeless clients or homeless individuals is indeed protected health information as defined in the HIPAA rules.

HIPAA standards take precedence over HMIS because HIPAA standards are finely attuned to the requirements of the health care system; they provide important privacy and security protections for protected health information; and it would be an unreasonable burden for providers to comply with and/or reconcile both the HIPAA and HMIS rules. This spares organizations from having to deal with the conflicts between the two sets of rules.

DATA POLICIES AND PROCEDURES

Data Quality

All data entered into HMIS must meet data quality standards. Participating Agencies will be responsible for their users' quality of data entry.

1. *Definition:* Data quality refers to the timeliness, completeness, and accuracy of information collected and reported in the HMIS.
2. *Data Timeliness:* End users must enter all universal data elements and program-specific data elements within three (3) days of intake.
3. *Data Completeness:* All data entered into the system is complete.
4. Data Accuracy: All data entered shall be collected and entered in a common and consistent manner across all programs.
    - Participating Agencies must sign the HMIS Agency Participation Agreement (Appendix A) to ensure that all participating programs are aware and have agreed to the data quality standards.
    - Upon agreement, Participating Agencies will collect and enter as much relevant client data as possible for the purposes of providing services to that client.
    - All data will be input into the system no more than three (3) days of program entry.
    - The HMIS staff will conduct monthly checks for data quality. Any patterns of error or missing data will be reported to the Participating Agency.
    - End users will be required to correct the identified data error and will be monitored for compliance by the Participating Agency and the HMIS staff.
    - End users may be required to attend additional training as needed.

Data Use and Disclosure

All end users will follow the data use Policies and Procedures to guide the data use of client information stored in HMIS.

Client data may be used or disclosed for system administration, technical support, program compliance, analytical use, and other purposes as required by law. Uses involve sharing parts of client information with persons within an agency. Disclosures involve sharing parts of client information with persons or organizations outside an agency.

- Participating Agencies may use data contained in the system to support the delivery of services to homeless clients in the continuum. Agencies may use or disclose client information internally for administrative functions, technical support, and management purposes. Participating Agencies may also use client information for internal analysis, such as analyzing client outcomes to evaluate program.
- The vendor and any authorized subcontractor shall not use or disclose data stored in HMIS without express written permission to enforce information security protocols. If granted permission, the data will only be used in the context of interpreting data for research and system troubleshooting purposes. The Service and License Agreement signed individually by the HMIS Lead Agency and vendor contain language that prohibits access to the data stored in the software except under the conditions noted above.

Data Release

All HMIS stakeholders will follow the data release Policies and Procedures to guide the data release of client information stored in HMIS.

Data release refers to the dissemination of aggregate or anonymous client-level data for the purposes of system administration, technical support, program compliance, and analytical use.

- No identifiable client data will be released to any person, agency, or organization for any purpose without written permission from the client.
- Aggregate data may be released without agency permission at the discretion of the Continuum. It may not release any personal identifiable client data to any group or individual.

Kansas Balance of State Continuum of Care

HMIS PRIVACY POLICIES AND PROCEDURES

The goal of the KS BOS COC Homeless Management Information Systems (hereafter "the HMIS") Privacy Policies and Procedures is to ensure confidentiality and security of all client data captured in the HMIS in conformity with all current regulations related to privacy and data confidentiality rights.

Outlined in this Kansas Balance of State HMIS Privacy Policy and Procedure are the Kansas Balance of State Continuum of Care (COC) standards and parameters to be followed by all HMIS Participating Agencies (PA). The COC recognizes its participating agencies may have established their own policies that meet HUD privacy requirements and the COC standards set forth herein. The Kansas Balance of State COC HMIS Privacy Policy and Procedure is not intended to supplant individual PA privacy policies. As long as PA privacy policies and practices meet the thresholds established in this policy and do not contradict the practices described, PAs may establish additional or more stringent requirements for HMIS end users. Additionally, this policy serves to describe how the HMIS Lead Agency and the Kansas Balance of State COC HMIS meet the privacy requirements established in HUD privacy standards.

POLICY ACCESS AND AMENDMENT

The HMIS Lead Agency may amend its privacy policy and practices at any time, subject to the recommendation of the HMIS Governance Committee. The HMIS Lead Agency may bring issues to the COC HMIS Committees, as necessary. An amendment may affect data that had been entered in the HMIS before the effective date of any such amendment. This policy is consistent with current privacy standards for HMIS issued by HUD.

The Privacy Policy will be reviewed and amended consistent with the procedure described in the Roles and Responsibilities section of the HMIS Policies and Procedures.

Applicability

The Kansas Balance of State HMIS Privacy Policy and Procedure applies to the HMIS Lead, PAs, and any person accessing HMIS data. PA projects subject to the privacy rules established under the authority of the Health Insurance Portability and Accountability Act (HIPAA) or other more restrictive policies will be honored.

The limitations of the HMIS implementation are described in the Client Informed Consent and Privacy Rights section of the HMIS Policies and Procedures.

The HMIS Lead Agency and PAs will uphold federal and state confidentiality regulations to protect client records and privacy. If a PA is covered by more stringent regulations, such as HIPAA, the more stringent regulations will prevail. Any project not subject to the Kansas Balance of State HMIS Privacy Policy and Procedure will be identified in the PA's HMIS Agency Participation Agreement.

PARTICIPATING AGENCY POLICY

Each PA is responsible for maintaining a privacy policy and certifying that each participating project complies with the Kansas Balance of State HMIS Privacy Policy and Procedure. PA Administrators are responsible for reviewing privacy policies and ensuring consistency with the Kansas Balance of State HMIS Privacy Policy and Procedure. At times, PAs may require more rigorous privacy standards, but they

must, at minimum, meet and not contradict the privacy standards set forth herein. In addition, PAs must maintain documentation regarding changes to their privacy policies.
Each PA will adopt the standard policy or their own, if the policy meets and does not contradict with the privacy standards set forth in this Policy and Procedure.

A PA's Privacy Policy will:

- Specify the purpose for collecting the information.
- Specify all potential uses and disclosures of client personal information.
- Specify the time for which the hard copy and electronic data will be retained at the organization and the method for disposing of it or removing identifiers from personal information that is not in current use.
- State the process and applicability of amendments and commit to documenting all amendments.
- Offer reasonable accommodations for persons with disabilities and/or language barriers.
- Allow the client the right to inspect and to have a copy of their client record and offer to explain any information the individual may not understand.
- Include reasons and conditions when an organization would not release information.
- Specify a procedure for accepting and considering questions or complaints about the privacy policy.

COMPLIANCE REVIEW

The HMIS Lead Agency is responsible for ensuring HMIS is operated in accordance with HUD standards. PAs are responsible for conducting annual reviews certifying each participating project complies with the Kansas Balance of State HMIS Privacy Policy and HUD standards. The Kansas Balance of State CCC, through the HMIS Lead Agency, retains the right to conduct site visits to ensure compliance with the Kansas Balance of State HMIS Privacy Policy and Procedure.

Each year, PAs will be required to self- certify that they comply with the Kansas Balance of State HMIS Privacy Policy and Procedure. PAs must indicate whether it has:

- Adopted the Kansas Balance of State HMIS Privacy Policy and Procedure, or
- Adopted a different privacy policy that meets the requirements outlined in the Kansas Balance of State HMIS Privacy Policy and Procedure.

In the event the PA adopts a different privacy policy, the PA will be expected to attach a copy of the policy to their HMIS Agency Participation Agreement. If no policy has been adopted at time of execution of the HMIS Agency Participation Agreement, or at the time of the annual certifications thereafter, the PA must establish a date no later than three months from the certification review date by which such a policy will be developed and implemented.

PRIVACY POLICY NOTICE

The HMIS Lead Agency and PAs must ensure privacy policies are readily accessible to clients and the public.

PUBLIC ACCESS PROCEDURE

The CoC will post the Kansas Balance of State HMIS Privacy Policy and Procedure on its official website and provide a copy to any individual upon request.

INFORMED CLIENT CONSENT PROCEDURE

The HMIS Lead Agency will maintain HMIS data using lawful and fair means. PA privacy policies will include a provision stating the PA will only collect data with the consent of their clients. Any client seeking assistance from a PA will be notified through a signed consent form that data collection will occur. The HMIS Lead Agency will assume that client information in the Kansas Balance of State HMIS has been entered with the consent of the client according to these policies and procedures. All PAs will keep copies of the signed consents on file. Individual PAs may maintain stricter policies relating to client consent to collect and share data with the HMIS Lead Agency.

At minimum, the COC requires PAs to post signs at each intake desk or other appropriate locations where data collection occurs explaining the reasons for HMIS data collection. The sign will include the following language:

> *"We collect personal information about individuals in a computer system called a Homeless Management Information System (HMIS) for reasons that are discussed in our privacy policy. We may be required to collect some personal information by organizations that fund the operation of this program. Other personal information that we collect is important to run our programs, to improve services for individuals, and to better understand the needs of individuals. To provide or coordinate individual referrals, case management, housing or other services, some client records may be shared with other organizations that are required to have privacy policies in place to protect your personal information.*
> *We only collect information that we consider appropriate. If you have any questions or would like to see our privacy policy, our staff will provide you with a copy. You have the right as a client to decline to share your information."*

Agencies may use the sample privacy notice attached in Appendix G of the HMIS Policies and Procedures.

ACCESSIBILITY PROCEDURE

Each PA that is a recipient of federal assistance will 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 organization.

PAs must make reasonable accommodations for persons with disabilities throughout the consent, intake, and data collection processes. This may include, but is not limited to, providing qualified sign language interpreters, readers, or materials in accessible formats such as Braille, audio, or large type as needed by the individual with a disability.

HMIS DATA USE AND DISCLOSURE

The confidentiality of HMIS data will be protected. PAs must collect data by legal and fair means, consistent with the Data Policies and Procedures section of the HMIS Policies and Procedures. The HMIS Lead Agency and PAs may only collect, use, and disclose data for the specific purposes and reasons defined in this section.

The HMIS Lead Agency collects HMIS data from organizations that directly enter data into the Kansas Balance of State HMIS System with the knowledge and authority of the COC HMIS Governing Committee. HMIS data may only be collected, used, or disclosed for activities described in this section.

The HMIS Lead Agency requires that PAs notify individuals seeking their assistance that data collection, use, and disclosure will occur. By entering data into the Kansas Balance of State HMIS System, the PA verifies that individuals have provided the PA with consent to use and disclose their data for purposes described below and for other uses and disclosures the HMIS Lead Agency determines to be compatible:

- To provide or coordinate individual referrals, case management, housing, or other services. Client records may be shared with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information.
- For functions related to payment or reimbursement for services.
- To carry out administrative functions, including but not limited to audit, personnel oversight, and management functions.
- To produce aggregate-level reports regarding use of services.
- To produce aggregate-level reports for funders or grant applications.
- To create de-identified (anonymous) information.
- To track system-wide and project-level outcomes.
- To identify unfilled service needs and plan for the provision of new services.
- To conduct a study or research project approved by the COC.
- When required by law (to the extent that use, or disclosure complies with and is limited to the requirements of the law).
- To avert a serious threat to health or safety if:
    - The use or disclosure is reasonably believed to be 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.
- To report about an individual reasonably believed to be a victim of abuse, neglect, or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect, or domestic violence in any of the following three 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 either of the following are applicable:
        i. The PA believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
        ii. 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 HMIS data 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;
    - When such a permitted disclosure about a victim of abuse, neglect, or domestic violence is made, the individual making the disclosure will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:
        i. In the exercise of professional judgment, it is believed that informing the individual would place the individual at risk of serious harm; or
        ii. It would be informing a personal representative (such as a family member or friend), and it is reasonably believed that 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 in the exercise of professional judgment.

- To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
    - In response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer, or a grand jury subpoena.
    - If the law enforcement official makes a written request for HMIS data that:
        i. Is signed by a supervisory official of the law enforcement agency seeking the HMIS data;
        ii. States that the information is relevant and material to a legitimate law enforcement investigation;
        iii. Identifies the HMIS data sought;
        iv. Is specific and limited in scope to the extent reasonably practicable considering the purpose for which- the information is sought; and
        v. States that de-identified information could not be used to accomplish the purpose of the disclosure.
- If it is believed in good faith that the HMIS data constitutes evidence of criminal conduct that occurred on the PA's premises.
- In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the HMIS data 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 HMIS data 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.
- To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.
- To third parties for the following purposes:
    - To permit other systems of care to conduct data matches (i.e., to determine if you are also utilizing services from such other systems of care); and
    - To permit third party research firms and/or evaluators to perform research and evaluation services, as approved by the COC, in connection with the projects administered by the HMIS Provided that before client-level HMIS data are disclosed under this subsection, the third party that will receive such client-level HMIS data and use it as permitted above must first execute a Data Use and Security Agreement (found in Appendix H of the Policies and Procedures). The Data Use and Security Agreements requires the third party to comply with all applicable laws and regulations, including the privacy standards and disclosure provisions contained in the current HUD HMIS Data and Technical Standards.

HMIS Lead Agency and the PAs

The HMIS Lead may share client level HMIS data with contracted entities as follows:

- The PA originally entering or uploading the data to the Kansas Balance of State HMIS.

- Outside organizations under contract with the HMIS Lead Agency or other entities acting on behalf of the Kansas Balance of State COC for research, data matching, and evaluation purposes. The results of this analysis will always be reported in aggregate form; client level data will not be publicly shared under any circumstance.

Entities providing funding to organizations or projects required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by the HMIS Lead Agency when there is a voluntary written agreement in place between the funding entity and the organization or project. In such cases, funder access to HMIS will be limited to data on the funded organization or project. Funding for any organization or project using HMIS cannot be contingent upon establishing a voluntary written agreement allowing the funder HMIS access.

Any requests for reports or information from an individual or group who has not been explicitly granted access to the Kansas Balance of State HMIS will be directed to the HMIS Governance Committee. No individual client data will be provided to meet these requests without proper authorization.

Before any use or disclosure of Personal Identifying Information (PII) that is not described here is made, the HMIS Lead Agency or PA wishing to make the disclosure will seek the consent of all individuals whose PII may be used or disclosed.

Access and Correction

Clients whose data is collected in HMIS may inspect and receive a copy of their HMIS record by requesting it from the PA that originally collected the information. The HMIS Lead Agency requires the PA to establish a policy to manage such requests and to explain any information a client may not understand.

Each PA privacy policy will describe how requests from clients for correction of inaccurate or incomplete HMIS records are handled. The policy will allow clients to request their HMIS data or request the data be removed from the HMIS. Nothing in this section is intended to indicate that a PA is released from any obligation by any funder to collect required data elements.

If a client requests to have his or her information in the HMIS corrected or removed, and the PA agrees that the information is inaccurate or incomplete, they may delete it or they may choose to mark it as inaccurate or incomplete and to supplement it with additional information. Any such corrections applicable to the data stored in the HMIS system will be corrected within one week of the request date.

If a client requests to view his or her data in the HMIS, the PA HMIS Administrator will keep a record of such requests and any access granted. The PA HMIS Administrator or PA Case Manager will provide a copy of the requested data within a reasonable timeframe to the client.

PAs are permitted to establish reasons for denying client requests for inspection of HMIS records. These reasons are limited to the following:

- If the information was compiled in reasonable anticipation of litigation or comparable proceedings
- If the record contains information about another client or individual (other than a healthcare provider or homeless provider) and the denial is limited to the section of the record containing such information

- If the information were obtained under a promise of confidentiality (other than a promise from a healthcare provider or homeless provider) and if the disclosure would reveal the source of the information
- Disclosure of the information would be reasonably likely to endanger the life or physical safety of an individual.

If a PA denies a request for access or correction, the PA will explain the reason for the denial. The PA will also maintain documentation of the request and the reason for the denial.

PAs may reject repeated or harassing requests for access to or correction of an HMIS record.

Data Retrieval and Sharing
HMIS, as implemented in the Kanas Balance of State COC, is a system that will generate reports required by HUD, the COC, and other stakeholders at a level that does not identify individuals but can provide accurate statistical data such as numbers served and trend assessments based on data entered by PAs. Data from the HMIS will be used to produce COC and local level statistical reports as well as corresponding reports. These purposes are included in the HMIS Data Use and Disclosure section of the HMIS Privacy Policies and Procedures.

The HMIS Lead Agency and COC Lead Agency staff have access to retrieve all data in the Kansas Balance of State HMIS. The HMIS Lead Agency and COC Lead Agency will protect client confidentiality in all reporting.

PAs may share PII with each other for the purposes of determining eligibility and coordinating client services once an agreed upon Release of Information is in place, as outlined in the Data Policies and Procedures section of the Policies and Procedures. PAs may also retrieve HMIS data entered to produce statistical reports including number of clients served and trend assessments for internal purposes, grant applications, and other required reports, within the parameters established by the COC HMIS Governance Committee.

GRIEVANCE
Concerns related to the Kansas Balance of State COC HMIS Privacy Policy and Procedure may be raised according to the procedures outlined in the HMIS Client Grievance Policy and Procedure. PAs must establish a policy and regular process for receiving and reviewing complaints from clients about potential violations of the policy.

PAs should report any violation of their privacy policy to the HMIS COC Governance Committee. In addition to any corrective actions taken by the PA, the HMIS Governance Committee may also report the findings to the HMIS Lead Agency or law enforcement, as appropriate, for further action. Such action may include, but is not limited to the following:
- Suspension of system privileges
- Revocation of system privileges

Individuals sanctioned because of HMIS privacy violations, can appeal to the COC HMIS Governing Committee. All HMIS end-users are required to comply with this privacy policy. PAs must ensure all end-users involved in HMIS data collection and/or entry receive privacy policy training. End users must receive and acknowledge receipt of this privacy policy.