Homeless Management Information System (HMIS) and Data Quality Policies & Procedures Manual

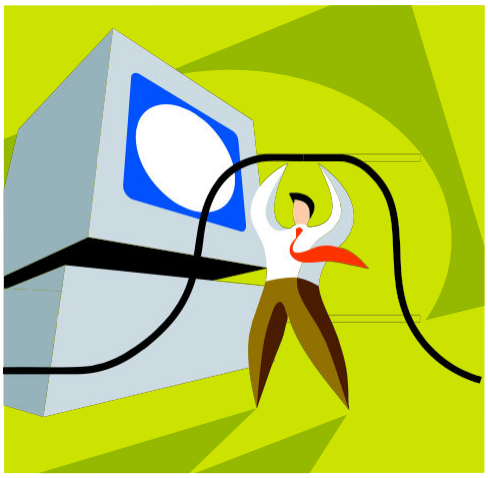

TABLE OF CONTENTS

1. **Introduction**

This document provides the framework for the ongoing operations of the Bakersfield-Kern Homeless Collaborative's (BKRHC or The Collaborative) Homeless Management Information System (HMIS). The Overview provides the main objectives, direction and benefits of HMIS. Governing Principles establish the values that are the basis for all policy statements and subsequent decisions.

Operating Procedures will provide specific policies and steps necessary to control the operational environment and enforce compliance in the areas of:

Participation
User Authorization
Collection and Management of Client Data
Release and/or Sharing of Client Data
Server Security and Availability
Workstation Security
Training
Technical Support

Other Obligations and Agreements will discuss external relationships required for the continuation of HMIS. Forms provides information on obtaining forms, filing and record keeping.

2. **Overview**

The long-term vision of HMIS is to enhance Voting Members' collaboration, with a view toward improving homeless service delivery and data collection capabilities. Accurate information will inform The Collaborative about homeless clients' needs, help in service gaps analysis, and strengthen needs-based funding requests.

The purpose of the BKRHC's HMIS is to help collect, analyze and report accurate, unduplicated client data on homeless and at-risk individuals and families served by a network of local homeless service providers in an effort to ensure the best possible service planning and delivery. This system is designed to meet the Federal mandates of the U.S. Department of Housing and Urban Development (HUD), which is a major funder of the BKRHC's Continuum of Care (CoC) programs to the homeless.

The fundamental goal of HMIS is to document the demographics of homelessness in Kern County according to the HUD HMIS Standards. It is then the goal of BKRHC to identify patterns in the utilization of assistance and document the effectiveness of the services for the client. This will be accomplished through analysis of data that is gathered from the actual experiences of homeless persons and the service providers who assist them in shelters and homeless assistance programs throughout the county. Data that is gathered via intake interviews and program participation (Coordinated Assessment) will be used to complete HUD Annual Progress Reports. This data may also be analyzed to provide unduplicated counts and anonymous aggregate data to policy makers, service providers, advocates, funders and consumer representatives.

HMIS utilizes a web-enabled application residing on a central server to facilitate data collection by homeless service organizations across the county. Access to the central server is limited to agencies formally participating in HMIS and then only to authorized staff members that meet the necessary training and security requirements.

Potential benefits for homeless men, women, and children: Customer service quality can be improved when client information is gathered according to HMIS' required Universal Data Elements and Workflows, which ensure that all the right questions get asked at intake and that no relevant client data gets missed. Also, when clients consent to having their information shared among intra/inter-agency staff, a truly tailor-

made Continuum of Care can be established for that client/family among all direct service providers.

Potential benefits for agencies participating in HMIS: Client information collected into a database dedicated to documenting the demographic trends and service needs of the local homeless population can avoid client duplication among partnering agencies and be used to effectively develop the best service plan possible. The data can also be used to measure and report program outcomes, which in turn can aid in advocacy and fundraising efforts with local policymakers, grantors and federal funding agencies such as HUD. Big volume shelter service providers can use HMIS in conjunction with scanning software and hardware to automate the data entry of such batch services as bed-nights, meals, showers, meds disbursements, etc., thereby saving many man hours of data entry work that would otherwise have to be performed manually.

Potential benefits for the community at large, including policymakers, grantors, and other stakeholders: Comprehensive Annual Progress Reports that reflect the local Continuum of Care's countywide efforts can assist in identifying specific service gaps in homeless services at multi-tiered urban and rural levels. Furthermore, other service reports required annually by HUD (such as the Annual Homeless Assessment Report; Housing Inventory Chart Report; Sheltered/Unsheltered Point-in-Time Count etc.) can be generated or supported by HMIS; these reports can then be used to inform policy decisions aimed at addressing and ending homelessness at the local, state and federal levels.

3. **Governing Principles**

Described below are the overall governing principles upon which all decisions pertaining to HMIS are based.

Participants are expected to read, understand, and adhere to the spirit of these principles, even when the Policies and Procedures Manual do not provide specific direction.

Confidentiality

The rights and privileges of clients are crucial to the success of HMIS. These policies will ensure clients' privacy without impacting the delivery of services, which are the primary focus of agency programs participating in this project.

Policies regarding client data will be founded on the premise that a client owns his/her own personal information. These policies will provide the necessary safeguards to protect client, agency, and policy level interests. Collection, access and disclosure of client data through HMIS will only be permitted by the procedures set forth in this document, which will be updated, as needed, following HUD guidance on data collection/client confidentiality requirements.

Data Integrity

Client data is the most valuable and sensitive asset of HMIS. These policies will ensure integrity and protect this asset from accidental or intentional unauthorized modification, destruction or disclosure.

System Availability

The availability of a centralized data repository is necessary to achieve the ultimate countywide aggregation of unduplicated homeless statistics. The HMIS Lead is responsible for ensuring the broadest deployment and availability for homeless service agencies in Kern County.

Compliance

Violation of the policies and procedures set forth in this document will have serious consequences. Any

deliberate or unintentional action resulting in a breach of BKRHC HMIS Policies & Procedures (per the Policies & Procedures Manual and/or Individual User Agreement) will result in a report by the HMIS Lead to the Governing Board for review and further action if any.

4. Roles and Responsibilities

Bakersfield-Kern Homeless Collaborative (Through its CoC Planning & Performance and BKRHC Governing Board)

- Approve and enforce all HMIS policies and procedures
- Retrieval and use of all or partial system-wide effectiveness data
- Considers and seeks additional funding to adequately support HMIS Project
- Encourages enrollment in HMIS among new BKRHC members

HMIS/Data Quality Committee

- HMIS Committee Make-up: HMIS Lead, Data Analyst, CoC Lead, and Committee Members/End Users
- HMIS participation with feedback to the BKRHC Governing Board
- Performance Review of service provider's APRs and Data Quality Control Checklist on a quarterly cumulative basis. Develop the Quarterly Performance Chart to facilitate the performance discuss in the CoC Performance Committee meeting for action taken for those providers falling short of COC Goals.
- Propose any changes to HMIS forms, documentation, or Policies and Procedures to the CoC Planning and Performance and Housing Committees for input with final review and approval by the BKRHC Governing Board.
- Provide HMIS direction and guidance to Participants
- Technology Plan including identifying HMIS needs and selection of system software
- Overall responsibility for success of HMIS
- Obtain necessary signatures for Memoranda of Understandings, Interagency Data Sharing Agreements and End User Agreements
- In compliance with the Charter and the HEART Act a bi-annual review of HMIS Policies, Procedures and Forms, will be conducted in accordance with The Hearth Act.

HMIS Lead

- HMIS Liaison with HUD
- Regular attendance of BKRHC Governing Board, HMIS/Data Quality, Housing and CoC Committee Meetings
- HMIS Staffing & HMIS Funding (Grant Management)
- Contingency Plan to be implemented in the absence of current HMIS Lead
- Creation of HMIS forms and documentation
- Review of and updates to HMIS Policies & Procedures and compliance issues
- Site Security Assessment
- HMIS Application Maintenance
  - Review vendor's plan on system backup and disaster recovery
  - System uptime, help desk and performance monitoring
  - Strive to ensure minimum disruption to end users during general system maintenance and upgrades
  - Ongoing protection of confidential data per HIPAA Policy
  - Procurement of Server Hosting and end user licenses
  - Adherence to HUD Data Standards
  - Application Customization
- End User Administration
  - Add and remove end users' rights to HMIS application

- Add and remove Voting Members Agency Primary Contact
- Outreach/End User Support

- Training
  - Application Training for Agency Administrators and End Users (System, Security, Privacy/HIPAA)

- Curriculum Development
- Training documentation
- Generate customize reports based on CoC and end user needs.

HMIS Data Analyst

- Extensive data analysis on local homelessness (demographic, economic, trend, and other data)
- Identification of gaps in data collection as required by HUD and/or the CoC
- Proper collection and submission of data per HUD and/or CoC requirements
- Dissemination of crucial information regarding HMIS system updates, as mandated by HUD, to both software providers and end users
- Accurate reporting of CoC, program or agency performance on a quarterly, semiannual and annual basis from HMIS to the CoC BKRHC Governing Board, and as needed in online-based HUD reporting tools or portals (for example, Homelessness Data Exchange (HDX), E-Snaps application and grant management system, etc.)
- Assistance with delivery of training to HMIS Database users
- Recruitment of agencies not currently using HMIS in order that more agencies can begin using this HUD-required system of data collection on local homelessness;
- Customization of data collection needs by agency
- Assistance with data and narrative to be incorporated into the annual CoC funding application to HUD
- Guidance on ways to improve data collection and quality per HUD and/or CoC requirements
- Attendance at monthly meetings of the HMIS/Data Quality Committee, BKRHC Governing Board, and other committees of the Homeless Collaborative, as required

Voting Members Agency (PA)

PA Executive Director

- Authorizing agent for MOU
- Designation of Agency Primary Contact and Agency Staff who will use HMIS
- Agency compliance with Policies & Procedures
- Periodic Review Agency End User licenses
- Agency level HUD reporting
- Confidentiality and HIPAA training

Agency Staff

- Safeguard Client Privacy through Compliance with security, confidentiality and HIPAA policies
- Data Collection as specified by training and other documentation.
- Timely submittal of Quarterly APRs and Data Quality Worksheets
- Submission of APRs in both PDF and Excel format to HMIS Lead and Data Analyst upon electronic submission to HUD
- Protect Username and passwords from being used inappropriately
- Adhere to the signed End User Agreement

5. OPERATING PROCEDURES

5.1 Participation

Policies

• Agencies participating in HMIS shall commit to abide by the governing principles of HMIS and adhere to the terms and conditions of this partnership as detailed in the Memorandum of Understanding.

Procedures

Confirm Participation

1. The Voting Members Agency shall confirm their participation in the HMIS Project by signing a Memorandum of Understanding.
2. The HMIS Lead will maintain a file of all signed HMIS Governance Documents.
3. The HMIS Lead will keep an updated list of all Voting Members and End Users.

Terminate Participation

Voluntary

1. The Voting Members Agency shall inform the HMIS Lead in writing of their intention to terminate their agreement to participate in HMIS.
2. The HMIS Lead will inform the HMIS Committee and update the Participating Agency List.
3. The HMIS Lead will revoke access of the Voting Members Agency staff to HMIS. Note: All Voting Members Agency-specific information contained in HMIS will remain in the system.
4. The HMIS Lead will keep all termination records on file with the associated Memoranda of Understanding.

Lack of Compliance

Violation of the policies and procedures set forth in this document will have serious consequences. Any deliberate or unintentional action resulting in a breach of BKRHC HMIS Policies & Procedures (per the Policies & Procedures Manual and/or Individual User Agreement) will result in a report by the HMIS Lead to the Governing Board and the CoC Planning & Performance Committee for review and further action if any. The HMIS Lead will report such a lack of compliance/violation of policies and procedures within 30 days of discovery.

Voting Members Agency Primary Contact

1. The Voting Members Agency shall designate a primary contact for communications regarding HMIS by submitting a Voting Members Agency Primary Contact Agreement form to the HMIS Lead.
2. The Voting Members Agency Primary Contact will inform the HMIS Lead regarding any new

HMIS End Users or those needed to be terminated.

Site Security Assessment

1. Prior to allowing access to the HMIS, the Voting Members Agency Primary Contact and the HMIS Lead will meet to review and assess the security measures in place to protect client data. This meeting will include Agency Executive Director (or designee), Program Manager/Administrator and Agency Technology Administrator and will assess agency information security protocols. This review shall in no way reduce the responsibility for agency information security, which is the full and complete responsibility of the agency, its Executive Director, and Agency Primary Contact.
2. Agencies shall have virus protection software on all computers that access HMIS.
3. Agencies must maintain the level of security instructed by HMIS Lead.

5.2 User Authorization & Passwords

Policies

- Agency Staff participating in HMIS shall commit to abide by the governing principles of HMIS and adhere to the terms and conditions of the HMIS End User Agreement.
- The Voting Members Agency Primary Contact must only request user access to HMIS for those staff members who have signed the HMIS End User Agreement.
- All users must have their own unique user ID and should never use or allow use of a user ID that is not assigned to them.
- Temporary, first time only, passwords will be communicated via email to the owner of the User ID.
- User specified passwords should never be shared and should never be communicated in any format.
- New User IDs must require password change on first use.
- Passwords must consist of at least 8 characters and must contain a combination of letters and numbers (no special characters; alpha and numeric only). The password must contain at least two numbers. [Required by software.] According to the HUD Data and Technical Standards Final Notice (May2010).
- Passwords must be changed every 60 days. If they are not changed within that time period, they will expire and the user will be locked out of the system.
- Agency Users and Voting Members Agency Primary Contacts passwords may be reset by the HMIS Lead or the Data Analyst.
- Five (5) consecutive unsuccessful attempts to login will disable the User ID until the account is reactivated by an Administrator Level System User.

Procedures

Workstation Security Assessment

1. Prior to requesting user access for any staff member, the Voting Members Agency Primary Contact will assess the operational security of the user's workspace.
2. Voting Members Agency Primary Contact will confirm that workstation has virus protection properly installed and that a full-system scan has been performed within the last week.
3. Voting Members Agency Primary Contact will confirm that workstation has and uses a hardware or software firewall.

Request New User ID

1. When the Voting Members Agency Primary Contact identifies a staff member that requires access to HMIS, a HMIS End User Agreement will be provided to the prospective User.
2. The Prospective User must read, understand and sign the HMIS End User Agreement and return it to the Voting Members Agency Primary Contact.
3. The Voting Members Agency Primary Contact will ensure the HMIS End User Agreement is signed by all relevant Voting Members Agency signatories and provide the signed original or a scanned copy to the HMIS Lead.
4. The HMIS Lead will co-sign the End User Agreement and provide a copy to the Voting Members Agency.
5. The HMIS Lead will create the new user ID as specified and notify the user ID owner of the temporary password via email.

Change User Access

1. When the Voting Members Agency Primary Contact determines that it is necessary to change a user's access level they will contact the HMIS Lead or Administrator Level System User to update the user ID as needed.

Rescind User Access

Voluntary: Use this procedure when any HMIS user leaves the agency or otherwise becomes inactive.

Compliance Failure: Violation of the policies and procedures set forth in this document will have serious consequences. Any deliberate or unintentional action resulting in a breach of BKRHC HMIS Policies & Procedures (per the Policies & Procedures Manual and/or Individual User Agreement) will result in a report by the HMIS Lead to the CoC Planning & Performance Committee for review and further action if any. The HMIS Lead will report such a lack of compliance/violation of policies and procedures within 30 days of discovery.

User/Agency failure to comply with guidance from the Governing Board may result in the HMIS Lead's deactivation of all applicable user access to the system.

Reset Password

1. When a user forgets their password or has reason to believe that someone else has gained access to their password, they must immediately notify their Voting Members Agency Primary Contact.
2. The Voting Members Agency Primary Contact will reset the user's password and notify the user of their new temporary password.

5.3 Collection and Entry of Client Data

Policies

- In order to capture accurate participant entry and exit dates in HMIS: all HMIS users are to enter client data into HMIS in a timely manner, preferably on the date of client

enrollment in the project. Client enrollment in programs are accounted for by the date the project provided the service or assessed the client for service. Each HUD funded project reviews and submits data on a quarterly basis to the CoC Performance Committee to avoid duplications and null values.

- Client enrollment entries/exits in HMIS from all HMIS users should be completed during the intake/exit process or as soon as possible within ten (10) working days.

- Additionally, all HMIS users will maintain records of the date of services provided on the day services began and also the date of exit on the date the client was exited from the program or as soon as possible within the next three (3) working days. All Universal and Program Data Elements from the HUD HMIS Data and Technical Standards should be collected and entered into HMIS subject to client written consent

    - Universal Data Elements shall be entered into HMIS as soon as possible after intake and no longer than ten (10) working days following intake
- Services may NOT be denied if client refuses to consent disclosure of data to HMIS or declines to state any information
- Client shall be given printout of all HMIS data and/or releases or disclosures relating to them upon written request and within ten (10) working days
- All releases or disclosures must be maintained for seven (7) years
- Other Client Data will be gathered according to the policies, procedures and confidentiality rules of each individual program
- Hard copy or electronic files will continue to be maintained according to individual program requirements, and according to the HUD HMIS Data and Technical Standards
- Any authorized data imports will be the responsibility of the participating agency in compliance with MOU Agreement and applicable federal guidelines
- Voting Members are responsible for the accuracy, integrity, and security of all their data input
- Aggregate data that does not contain any client specific identifying data may be shared with internal and external agents without specific permission. This policy should be made clear to clients as part of the Intake process
- Each Agency Executive Director is responsible for their agency's internal compliance with the HUD Data Standard

Procedures

• Refer to HMIS User's Manual and/or Training Materials for specific data entry guidelines.

5.4 Release and Disclosure of Client Data

Policies

- Client-specific data from the HMIS system may be shared with Voting Members only when the sharing agency has secured an unexpired Release of Information from that client authorizing such sharing
- Sharing of client data may be limited by program specific confidentiality rules
- Note that services may NOT be denied if client refuses to sign Release of Information or declines to state any information
- Release of Information must constitute INFORMED consent and the burden rests with the intake counselor to inform the client before asking for consent
- All external releases or disclosures must be maintained for seven (7) years and made available to the client upon written request and within ten (10) working days

Procedures

- Procedures for disclosure of client-specific data are readily obtained from the above policies, combined with the configuration of the HMIS system, which facilitates appropriate data sharing.

5.5 Data Retention

Policies

- Since Client Data is held off-site on a hosted server and the price of storage is inexpensive there will be no need to dispose of any client data. These procedures will a give the CoC an opportunity to look at historical data without time gaps in client services and unnecessary duplicated records.
- All procedures for data removal are the responsibility of the HMIS Lead and Application Vendor.

5.6 Server Security

Policies

- The HMIS Lead will periodically review the vendor's methodology of securing the cloud based hosted servers, both physically and electronically.

Procedures

- All procedures for reviewing HMIS Server Security are the responsibility of the HMIS Lead.

5.7 Server Availability

Policies

- The HMIS Lead work with the HMIS vendor to strive to maintain continuous availability of the system according to best business practices and standards.
- Necessary and planned downtime will be scheduled when it will have least impact, for the shortest possible amount of time, and only after timely communication to all participants.
- HMIS Lead is responsible to work with the vendor in design and implementation of a backup and recovery plan (including disaster recovery).

Procedures

- A user should immediately report unplanned downtime to their Agency Primary Contact.
- All other procedures for maximizing Server Availability, recovering from unplanned downtime, communicating, and avoiding future downtime are the responsibility of the HMIS Lead.
- HMIS Lead will work with the HMIS vendor in forming a backup schedule of the system, software, and database data (on a weekly basis), as well as incremental backups nightly.

5.8 Workstation Security

Policies

- Voting Members Agency Primary Contact is responsible for preventing degradation of the whole system resulting from viruses, intrusion, or other factors under the agency's control.
- Voting Members Agency Primary Contact and Users are responsible for preventing inadvertent release of confidential client-specific information. Such release may come from physical or electronic or even visual access to the workstation, thus steps should be taken to prevent these modes of inappropriate access (i.e. don't let someone read over your shoulder; lock your screen).
- All workstations to be used with HMIS must be secured by a firewall between the workstation and the internet. Software firewalls are acceptable.
- Definition and communication of all procedures to all Agency users for achieving proper agency workstation configuration and for protecting their access by all Agency users to the wider system are the responsibility of the Voting Members Agency Primary Contact.

Procedures

- At a minimum, any workstation accessing HMIS shall have anti-virus software with current virus definitions (24 hours) and frequent full-system scans (weekly).

5.9 Training

Policies

- Agency Executive Director shall commit designated Staff to attend training as specified in the HMIS End User Agreement or recommended by the HMIS Lead.

Procedures

Start-up Training

HMIS Lead will schedule and provide training in the following areas to Voting Members Agency using HMIS:

- Agency Primary Contact Training
- End User Training
- Confidentiality and HIPAA Training

Voting Members Agency Primary Contact Training

Training will be done in a group setting, where possible to achieve the most efficient use of time and sharing of information between agencies. Training will include:

- Requests for New user set-up
- Assigning Agency within HMIS hierarchy.
- End user training
- Running package reports
- Creating customized reports

Follow-up Training

HMIS Lead will provide on-site follow-up training at each participating Voting Members. Once a new Voting Members Agency has "gone live," the HMIS Lead will make on-site visits as requested to ensure that the Voting Members Agency becomes proficient in the use of HMIS.

Ongoing Training

HMIS Lead and/or Data Analysis will provide regular training for the Continuum of Care, as needed. The areas covered will be:

- Agency Primary Contact Training
- End User Training
- Confidentiality and HIPAA Training

Additional training classes will be scheduled as needed. The monthly trainings will be posted on the Bakersfield-Kern Homeless Collaborative (BKRHC) Website Calendar. Usually the trainings are scheduled for the last Friday of the month every month unless the lab is being used for other scheduled training.

5.10 Technical Support

Policies

- Support Requests include problem reporting, requests for enhancements (features), or other general technical support.
- Users shall discuss support requests with their Voting Members Agency Primary Contact
- Users may submit support questions to the vendor via the help form in the HMIS application.
- Users should avoid calling the vendor directly without first going through the help desk submittal form process.
- Users shall not submit requests directly to the software vendor's Client Advocate without specific invitation or knowledge of the HMIS Lead and Data Analysis. All requests to the HMIS or Data Analyst may then be escalated to vendor as appropriate.
- HMIS Committee will only provide support for issues specific to the HMIS software and systems.
- Recommended Internet Connection: DSL or Cable Modem, at least 128 kbs.
- Recommended Browser: Latest release of Internet Explorer version 11. All other browsers are supported by the application and now can be used with the application.

Procedures

Submission of Support Request

1. User encounters problem or originates idea for improvement to system or software.
2. User creates Support Request via Help Desk Submittal Form found in the HMIS software specifying the severity of the problem and its impact on their work, specific steps to reproduce the problem, and any other documentation that might facilitate the resolution of the problem. User shall also provide contact information and best times to reach.
3. HMIS Lead or Data Analyst, upon receipt of a Help Desk Submittal Form, shall make reasonable attempts to resolve the issue.
4. If the HMIS Lead or Data Analyst is unable to resolve the issue and determines that the problem is specific to HMIS software and systems, they shall consolidate multiple similar requests and submit a Vendor Support Request by following the instructions found in the application.

   Note: If the Support Request is deemed by HMIS Lead to be an agency-specific customization[1], resolution of the request may be prioritized accordingly. HMIS

Lead/Data Analyst/Software Vendor reserves the right to charge on an hourly basis for these changes if/when the workload for such agency-specific customizations becomes burdensome.

5. HMIS Lead may at this point determine that the cause of reported issue is outside the scope of control of the HMIS software and systems.
6. HMIS Lead will consolidate such requests from multiple Voting Members, if appropriate, and strive to resolve issues in priority order according to their severity and impact.
7. If the HMIS Lead is unable to resolve the issue, other software or system vendor(s) may be included in order to resolve the issue(s).
8. In cases where issue resolution may be achieved by the end user or other Voting Members Agency personnel, HMIS Lead will provide instructions via email to Voting Members Agency Primary Contact user creating the original request.

1 Agency-specific customizations include but are not limited to new assessments, new data fields, and new pick lists.

5.11 Changes to the Manual and other Documents

Policies

• The CoC Performance Committee, HMIS/Data Quality Committee, and any ad hoc subcommittee thereof will guide the compilation and amendment of these Policies and Procedures.

Procedures

Changes to Policies & Procedures

1. Proposed changes may originate from any HMIS participant, or by the Leadership of the BKRHC, including the HMIS Lead, in response to newly established HUD, HIPAA, etc. requirements.
2. When proposed changes originate within a Voting Members Agency, they must be reviewed by the Voting Members Agency Executive Director, and then submitted via email to HMIS Lead for review and discussion in a scheduled HMIS/Data Quality Committee meeting.
3. HMIS Lead will maintain a list of proposed changes.
4. The list of proposed changes will be discussed by the HMIS/Data Quality Committee subject to line item excision and modification. This discussion may occur either at a meeting of the HMIS/Data Quality Committee or via email or conference call, according to the discretion and direction of the HMIS/Data Quality Committee.
5. Results of said discussion will be communicated, along with the amended Policies and Procedures. The revised Policies and Procedures will be identified within the document by the date of the HMIS/Data Quality Committee discussion.
6. Voting Members Executive Directors shall acknowledge receipt and acceptance of the revised Policies and Procedures within 15 working days of delivery of the amended Policies and Procedures by notification in writing or email to HMIS Lead. The Voting Members Agency Primary Contact shall also ensure circulation of the revised document within their agency and compliance with the revised Policies and Procedures.

6. Other Obligations and Agreements

The current HUD grant for HMIS provides for a limited number of user licenses. While it may not be possible to meet every agency's full requirements for licenses within the HUD grant to the Collaborative, the HMIS Lead will endeavor to make sure that every agency participating will meet HUD minimum requirements. Any funding needed for additional licenses will be determined by the HMIS Lead and communicated to the BKRHC's BKRHC Governing Board for appropriate action.

6.1. Data and Technical Standards

This document should, at a minimum, reflect the baseline requirements listed in the HMIS Data and Technical Standards Final Notice, published by HUD in May 2016 and in accordance with the HEARTH Act. Users of HMIS are required to read and comply with the HMIS Data and Technical Standards. Failure to comply with these standards carries the same consequences as does failure to comply with these Policies and Procedures. In any instance where these Policies and Procedures are not consistent with the HMIS and Data Quality Standards from HUD, the HUD Standards take precedence. Should any inconsistencies be identified, notice should be made to the HMIS Lead.

6.2. Health Insurance Portability and Accountability Act (HIPAA)/Violence Against Women Act (VAWA)

For agencies or programs where HIPAA/VAWA applies, HIPAA/VAWA requirements take precedence over both the HUD HMIS Data Requirements (as specified in those requirements) and these policies and procedures. Those agencies who are not required to use HMIS may have a parallel system to report and collect data per HUD's standards. However, they are still subject to the policies and procedures that are not specific to HMIS such as data quality.

7. Forms

All forms approved and required by the HMIS/Data Quality policies and procedures will be made available by the HMIS Lead in PDF format.

Filing of Completed Forms

ID	Description	Location	Responsibility
200-061703 MOU	Memorandum of Understanding	Collaborative	Project Manager
300-013103 INDSA	Interagency Network Data Sharing Agreement	VMA	Agency Admin
125-031203 ROI	Client Informed Consent & Release of Information Authorization	VMA	Agency Staff
400-073113 EUA	End User Agreement	Agency	Agency Staff